Tommi Saranpää

AALTO-YLIOPISTON VERKKOPALVELUIDEN ARKKITEHTUURI

Elektroniikan, tietoliikenteen ja automaation tiedekunta

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi diplomi-insinöörin tutkintoa varten Espoossa 25.5.2010.

Työn valvoja:

Prof. Heikki Hämmäinen

Työn ohjaaja:

DI Petri Makkonen

AALTO-YLIOPISTO
TEKNILLINEN KORKEAKOULU

DIPLOMITYÖN
TIIVISTELMÄ

Tekijä: Tommi Saranpää

Työn nimi: Aalto-yliopiston verkkopalvelujen arkkitehtuuri

Päivämäärä 25.5.2010 Kieli: Suomi Sivumäärä: 8 + 63

Elektroniikan, tietoliikenteen ja automaation tiedekunta

Tietoliikenne- ja tietoverkkotekniikan laitos

Professuuri: Tietoverkkotekniikka Koodi: S-38

Valvoja: Prof. Heikki Hämmäinen

Ohjaaja: DI Petri Makkonen

Tutkimuksessa vertaillaan kahta erilaista arkkitehtuurimallia Aalto-yliopiston verkon rakenteeksi. Tavoitteena on löytää arkkitehtuurimallien eroavaisuuksien vaikutuksia verkkopalveluiden toteuttamiseen ja käyttäjän kokemaan palveluvalikoimaan. Verkon arkkitehtuuri vaikuttaa käyttäjän kokemaan palveluun erityisesti ongelmatilanteissa. Verkkopalveluiden pitäisi Aalto-yliopiston kaltaisessa tekniikan, talouden ja taiteen ylintä opetusta antavassa yliopistossa olla esimerkkinä muille.

Tutkimuksessa on tarkoituksella valittu ääripään toteutusmallit. Ensimmäinen arkkitehtuurivaihtoehto on moderni operaattoriverkko. Siinä uusimmista tekniikoista otetaan kaikki irti ja tavoitteet on asetettu mahdollisimman korkealle.

Toisessa mallissa verkon rakenne on mahdollisimman yksinkertainen, mutta kuitenkin varmistettu kaksinkertaisilla yhteyksillä. Laitteiden hinta on kohtuullinen ja verkko on helppo ymmärtää.

Verkon toteuttamiseen on paljon vaihtoehtoja ja tämä tulee esiin tutkimukseen tehdyissä haastatteluissa. Eri asiantuntijoilta saa toisaalta hyvin samanlaisia ideoita ja toisaalta lähestymistavat ovat perinteisen varovaisia. Tutkimus toteutettiin kirjallisuus- ja haastattelututkimuksena. Haastateltaville lähetettiin kaaviokuva verkon rakenteesta, kampuksille menevistä yhteyksistä ja lista kysymyksistä etukäteen. Keskustelut olivat hyvin antoisia ja toivat uusia näkökulmia toteutusvaihtoehtoihin.

Tutkimuksen perusteella hajautettu malli antaa paljon mahdollisuuksia. Monipuolisten ominaisuuksien tuomaa hyötyä on vaikea mitata ja verrata kustannuksiin. Keskitetyn mallin valinta ei aiheuta lisäkustannuksia, jos myöhemmin siirrytään hajautettuun malliin.

Avainsanat: Verkkoarkkitehtuuri, reititys, hajauttaminen, keskittäminen, verkkopalvelu, varayhteys, valopolku

AALTO UNIVERSITY
SCHOOL OF SCIENCE AND TECHNOLOGY

ABSTRACT OF THE
MASTER'S THESIS

Author: Tommi Saranpää

Title: The Architecture of Aalto University's network services

Date 25.5.2010 Language: Finnish Number of pages: 8 + 63

Faculty of Electronics, Communications and Automation

Department of Communications and Networking

Professorship: Networking Code: S-38

Supervisor: Prof. Heikki Hämmäinen

Instructor: M.Sc. (Tech.) Petri Makkonen

This thesis compares two different models for Aalto University's network architecture. Their influence for producing network services and service portfolio that the users receive. Network architecture affects users' lives especially when there are problems in the network. Network services in a University giving the highest education of Arts, Economics and Technology should be as an example to others.

In the study the models of network architecture we intentionally chosen to be in the opposite ends of the line. The first model describes modern operator network including all the latest technologies. The goal is set as high as it can be. The second model is as simple, affordable and easy to understand as possible. Still every connection to campuses has been protected with secondary connection. The equipment is relatively cheap and the network easy to comprehend.

There are many alternatives to build a network like this. This comes up also in the inter views made for this study. Different experts give very similar answers and on the other hand the solutions are rather traditionally careful. The study was conducted as a documentation research and interviews. The interviewees were sent a document describing the network structure, network links to the campuses and a list of questions beforehand. The conversations were very interesting in useful and they gave many new ideas.

The study shows that the architecture with distributed routing gives plenty of opportunities, but the benefits compared to the extra costs are not easy to prove. The architecture with centralized routing is path leads to the architecture of distributed routing if necessary and without extra cost.

Keywords: network, architecture, distributed, centralized, routing, consolidating, services, lightpath

Esipuhe

Kiitos diplomityön valvojalle professori Heikki Hämmäiselle rakentavasta ja kannustavasta palautteesta. Ohjeet ja neuvot ovat tulleet nopeasti ja voin vain toivoa muille opiskelijoille samanlaista etuoikeutta heidän keskustellessaan opinnäytetöiden etenemisestä. Kiitos diplomityön ohjaajalle, diplomi-insinööri Petri Makkoselle. Meillä on ollut jo vuosien yhteistyö verkkojen rakentamisessa.

Perheeni on ollut myös hengessä mukana. Vaimoni Pia ja lapset Oona, Vilma, Konsta ja Aapo ovat olleet ymmärtäväisiä. Olen saanut sopivan rauhalliset puitteet kirjoittamiselle ja sen vastapainoksi onnellista yhdessäoloa ja perhe-elämää.

Kiitos asiantuntijoille Otto Kaipio (HP), Leo Lähteenmäki (Cisco) ja Juha Oinonen (CSC), joita sain haastatella diplomityöhöni. Heiltä sain vahvistusta käsityksiini, uusia ideoita ja syitä tarkistaa ajatuksiani uudestaan.

Kiitos sukulaisille ja ystäville, jotka ovat jaksaneet muistuttaa opiskelujen loppuunsaattamisesta. Opiskelun loppukiri oli kova ja samaan aikaan työtahti Aalto-yliopiston IT-palvelukeskuksessa oli hurja. Tähän kun yhdistetään vielä omakotitalon rakennustyömaa, niin harrastuksia ei enää tarvinnut miettiä.

Diplomityön aihe oli mielenkiintoinen ja kirjoittamisen aikana sain hyvän tilaisuuden syventyä MPLS:n mahdollisuuksiin yliopistomaailmassa. Löysin aivan uusia vaihtoehtoja perinteisestä verkonrakennuksesta.

Otaniemi, 24.5.2010

Tommi Saranpää

Lyhenteet

802.1X	Porttiautentikointi
BFD	Bidirectional Forwarding Detection protocol
CWDM	Coarse Wavelength-Division Multiplexing
DHCP	Dynamic Host Configuration Protocol
FC	Fibre Channel
GE	Gigabit Ethernet
GLBP	Gateway Load Balancing Protocol (Ciscon oma protokolla)
H.323	Videoneuvotteluprotokolla
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPSec	Internet Protocol Security
IPTV	Internet Protocol Television
iSCSI	Internet Small Computer System Interface
LACP	Link Aggregation Control Protocol (IEEE 802.3ad)
LDP	Label Distribution Protocol
LSP	Label Switched Path
MC-LAG	Multi-chassis link aggregation group
MPLS	Multiprotocol Label Switching
OAM	Operations, Administration and Management
P2MP	Point to Multipoint
PE	Provider Edge
RSVP	Resource Reservation Protocol
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol

TE	Traffic Engineering
UPS	Uninterruptible Power Supply
VLAN	Virtual LAN (IEEE 802.1Q)
VPLS	Virtual Private LAN Service
VRF-lite	VPN Routing and Forwarding lite
VRRP	Virtual Router Redundancy Protocol
WebDAV	Web-based Distributed Authoring and Versioning
VPN	Virtual Private Network
L2TP	Layer 2 Tunneling Protocol

Sisällysluettelo

1 Johdanto

1.1 Tutkimuksen tausta

Aalto-yliopiston [1] muodostaneiden kolmen korkeakoulun verkkopalveluiden yhdistäminen ja uusien palveluiden suunnittelu aloitettiin vuoden 2008 alussa. Toimeen ryhdyttiin pian sen jälkeen, kun Suomen hallitus oli tehnyt periaatepäätöksen Innovaatioyliopiston [2] perustamisesta. Valmisteluita vaikeutti tulevan yliopiston johdon ja tahdon puuttuminen. Kukaan ei tiennyt, miten Aalto-yliopisto tulisi järjestäytymään ja esimerkiksi millaisia verkkopalveluita tarvitaan kolmen vuoden kuluttua.

IT-palvelukeskus [3] on Aalto-yliopiston IT-palveluita tuottava yksikkö. Tehtäviin kuuluvat peruspalvelut opiskelijoille ja henkilökunnalle. Peruspalveluita ovat tietoliikenne, työasemapalvelut, levyjärjestelmät, varmuuskopiointi ja palvelimien ylläpito.

IT-palvelukeskus joutui itse suunnittelemaan ja miettimään tarvittavat palvelut. Suunnittelu oli hajanaista ja sitä tehtiin muun työn ohella. Verkon suunnitteluun käytettiin apuna ulkopuolista konsulttiyritystä. Suunnitteluavun hyödyllisyydestä ollaan erimielisiä, mutta suunnitelmat saatiin valmiiksi ja niiden mukaan on toimittu.

Verkon suunnittelun aikana ja sen jälkeen on suunniteltu muita välttämättömiä palveluita. Levyjärjestelmä, levypalvelu, palvelimet, työasemaympäristö, lupahallinto ja tulostusjärjestelmä ovat esimerkkejä näistä järjestelmistä. Jälkeenpäin on kritisoitu opiskelijoiden ja hallinnon järjestelmien myöhäistä suunnittelua ja käyttöönottoa. Ongelma niissäkin oli, että kukaan ei voinut päättää asioita tulevan yliopiston puolesta.

HSE:n ja TKK:n yhteinen tietohallinnon johtoryhmä [4] aloitti toimintansa vuoden 2008 alussa. Sen tavoitteena oli saada molempien korkeakoulujen ääni kuuluviin tietojärjestelmien suunnittelussa ja edistää yhteistyötä alusta asti. Taideteollisen korkeakoulun edustusta ei vielä tuolloin saatu mukaan. Tietohallinnon johtoryhmältä odotettiin linjauksia kaikesta tietotekniikkaan liittyvästä. Erilaisia periaatepäätöksiä valmisteltiin ja niitä saatiin hyväksyttyäkin useita. Esimerkkeinä voidaan mainita levypalvelinhankinta, työasemapolitiikka [5] ja älypuhelinpolitiikka. Kaikki politiikat määriteltiin siten, että palvelun toimittajaa ei rajata mitenkään. Niissä lueteltiin vain toimittajan vastuut.

Kolmen korkeakoulun yhteinen IT-palvelukeskus aloitti toimintansa 1.9.2008. Sen rinnalla toimi tietohallinto, jonka tehtävä oli suunnitella ja tilata IT-palveluita yliopistoa varten. Palveluita voi tilata joko IT-palvelukeskukselta tai ulkopuoliselta toimijalta. Henkilökunta siirtyi tehtävien mukaan joko IT-palvelukeskukseen tai tietohallintoon.

1.2 Tutkimusongelma

Aalto-yliopistolta ja sen verkkopalveluilta odotetaan paljon ja niiden odotusten lunastamiseksi on toimittava määrätietoisesti ja rohkeasti. Verkkoon liittyvien palveluiden suunnitteluun pitää käyttää riittävästi resursseja, että vaatimukset, laatu ja hinta kohtaavat. Tarpeet eivät vaihtele perusasioissa niin paljoa laitoksittain, että yhteisiä palveluita olisi mahdoton järjestää. Suurin haaste on löytää kompromissi ja saada kaikki osapuolet luopumaan vanhoista järjestelmistään. Osa laitoksista [6] on tottunut hoitamaan kaiken itse ja niiden voi olla hyvin vaikeaa luopua nykyisistä tehtävistä, vaikka niiden tekeminen laitostasolla ei olisikaan järkevää.

Tutkimuksessa [7] tarvitaan verkkoja ja laitteita joita ei ole syytä sekoittaa jokapäiväiseen tietokoneen ja verkon käyttöön. Tämän vuoksi tutkimusverkot on tarkoituksella pidetty riippumattomina tuotantoverkoista. Tutkimusverkoissa tutkijat voivat vapaasti ja turvallisesti tutkia eikä tuotannon koneiden ja palvelinten vaarantumista tarvitse miettiä.

Tässä tutkimuksessa selvitetään ja vertaillaan vaihtoehtoja verkkopalveluiden arkkitehtuuriksi. Tärkein tutkimuskohde on fyysisen verkon rakenne. Millaisia palveluita on olemassa ja odotettavissa ja millaista verkkoa ne tarvitsevat? Vastaavasti miten henkilökunnan työasemille ja kannettaville tietokoneille saadaan tarjottua nopeat ja luotettavat verkkoyhteydet, levy- ja tulostuspalvelut? Opiskelijoille tarvitaan tietokoneluokkia ja langaton verkko omien koneiden käyttämiseksi. Langatonta verkkoa pitäisi pystyä hyödyntämään myös henkilökunnan kannettavissa joustavasti.

Yhdistämällä verkon ylläpito, työasemien ja palvelinten ylläpito yhdeksi, koko yliopiston laajuiseksi järjestelmäksi antaisi mahdollisuuden tehostaa ja järkeistää IT-palveluita. Keskitetyn järjestelmän on tuettava mahdollisuutta delegoida ylläpito laitoksien ja tiedekuntien ylläpitäjille. Keskitetyn hallintajärjestelmän suosio Aalto-yliopistossa riippuu siitä, kokevatko laitoksien ylläpitäjät saavansa etua järjestelmästä. Keskitetysti kannattaa hoitaa perusasiat,

joita kaikkien ei tarvitse tehdä. Laitosten ylläpitäjät voivat keskittyä oman alansa sovelluksiin ja palveluihin.

Laitosten perustarpeet ovat hyvin samanlaisia. Kaikille työntekijöille tarvitaan:

- Riittävä tallennuskapasiteetti verkkolevyillä
- Nopea verkko
- Valmiit käyttöjärjestelmien sekä sovellusten asennusvaihtoehdot

Näiden vakioitujen perusasioiden päälle laitosten on helppo rakentaa omia tarpeitaan vastaavia palveluita.

1.3 Tutkimuksen rajaus

Tutkimus rajataan koskemaan verkkoa ja sen palveluita. Kampusten väliset yhteydet, protokollat ja verkkolaitteet kuvataan toiminnallisella tarkkuudella. Erityisesti eri vaihtoehtojen tuomat edut ja rajoitukset pyritään saamaan esiin. Tutkimuksessa rajoitutaan tutkimaan Ethernet-pohjaisia [8] ratkaisuja verkon toteuttamiseen. Tämä rajaus perustuu vakiintuneeseen laitekantaan ja kustannuksiin.

Tutkimuksessa pyritään löytämään olennaiset asiat verkon palveluista ja niiden tarpeista. Tämän vuoksi käsitellään verkkoa kampusten tasolla. Kampuksien sisällä toiminta on hyvin samanlaista ja suurin ero onkin maantieteellinen etäisyys.

1.4 Tutkimusmenetelmä

Tutkimusmenetelminä ovat kirjallisuustutkimus ja asiantuntijahaastattelut. Kirjallisuudessa tutkitaan erityisesti merkittävien laitevalmistajien parhaita käytäntöjä (Best Practices) ja alan uusimpia julkaisuja. Haastatteluissa on pyritty löytämään henkilöitä, joilla on näkemystä erilaisten verkkojen rakentamisesta ja heiltä on kysytty mielipiteitä ratkaisuista.

Haastatteluista on koostettu oma kappaleensa, jossa haastateltavien mielipiteitä analysoidaan ja verrataan muiden haastateltavien mielipiteisiin sekä ehdotettuihin toimintamalleihin. Haas-

tatelluille esitetään samat kysymykset, mutta keskustelua ja kommentointia ei rajoiteta mitenkään. Haastatelluilta halutaan saada ajatuksia ja ideoita joita ei ole osattu lainkaan huomioida.

1.5 Tutkimuksen rakenne

Diplomityössä on teoriaosa ja käytännön tutkimusosa. Ensimmäisessä luvussa on johdanto, joka kuvaa tutkimuksen taustan, tutkimusongelman, tutkimuksen rajauksen, tutkimusmenetelmän ja tutkimuksen rakenteen. Toisessa luvussa kuvataan palveluvalikoima, sen asettamat vaatimukset ja tulevaisuuden mahdollisuudet verkkopalveluille.

Teoriaosuus alkaa kolmannesta luvusta, jossa kuvataan yliopistolle välttämättömien IT-palveluiden toimintaa. Tutkimus alkaa kahdeksannesta luvusta, jossa analysoidaan olemassa olevaa verkkoa ja sen rajoituksia. Yhdeksännessä ja kymmenennessä luvuissa käsitellään vaihtoehtoisia toimintamalleja. Yhdennessätoista luvussa analysoidaan haastattelujen pohjalta saatuja tuloksia ja pohditaan miten niitä voidaan hyödyntää.

Diplomityön tavoitteena on kuvata Aalto-yliopiston tärkeimmät tietoverkkoa hyödyntävät palvelut ja verrata kahta erilaista verkkoratkaisua niiden toteuttamiseksi. Yliopistoverkon rakentamiseen on paljon vaihtoehtoja, joista tässä työssä vertaillaan kahta ääripäätä. Edullisimmassa mallissa reititys keskitetään kahteen konesaliin. Toisessa mallissa reititys hajautetaan kampuksille ja hyödynnetään viimeisimpiä tietoliikenteen tekniikoita.

Aalto-yliopiston muodostaneiden kolmen korkeakoulun tietojärjestelmät olivat hyvin erilaiset. Ainoastaan valtion tilivirastoille yhteisissä hallinnon järjestelmissä oli samoja sovelluksia. Niitäkin oli käytetty eri tavoin eikä tietojen yhdistäminen ollut yhdenkään osalta suoraviivaista. Verkkotekniikat olivat myös erilaisia ja niiden yhdistäminen Aalto-yliopiston yhteiseksi verkoksi ei ole ollut helppoa.

2 Palveluvalikoima

2.1 IT-palvelut henkilökunnalle ja opiskelijoille

Henkilökunnalle ja opiskelijoille tarjotaan monipuolinen valikoima palveluita ja ohjelmistoja. Suuri osa ohjelmistoista on kampussopimuksia tai kelluvia lisenssejä. Niiden kustannukset ovat edullisempia eikä sisäiseen laskutukseen kulu ylimääräistä rahaa. Esimerkkeinä keskeisistä ohjelmistoista ovat taulukon 1 ohjelmistot.

Matlab	http://www.mathworks.com/
Mathematica	http://www.wolfram.com/
Maple	http://www.maplesoft.com/
Mathcad	http://www.ptc.com/
Autocad	http://www.autodesk.fi/
Adobe Master collection	http://www.adobe.com/
COMSOL Multiphysics	http://www.comsol.com/
Microsoft Office	http://www.microsoft.com/
SSH	http://www.ssh.com/ tai http://www.openssh.org/

Taulukko 1 Keskeisiä ohjelmistoja

IT-palvelukeskus tarjoaa maksutta keskitetyn työasemaympäristön. Tietokoneista, tulostimista, värimonitoimilaitteista ja puhelimista on suositusmallit ja niille nopeat toimitusajat. Tavoite on ohjata hankintoja laadukkaampiin ja sitä kautta kokonaistaloudellisiin valintoihin. Pelkästään jo laitemallien määrän vähentyminen tuo kustannussäästöjä.

Palvelu	Palvelun tyyppi
Henkilökunnan työasemat	Peruspalvelu
Opiskelijoiden työasemat	Peruspalvelu
Tulostuspalvelu	Laitos maksaa laitteen, paperit ja värit
Yleispalvelimet	Peruspalvelu
Sähköposti, kalenteri, yhteystiedot ja tehtävälista	Peruspalvelu
Kotisivutila	Peruspalvelu
Wiki	Peruspalvelu

Palvelu	Palvelun tyyppi
Kotihakemisto henkilökohtaisille- ja asetustiedostoille	Peruspalvelu. Levykiintiö 5 Gt.
Työhakemisto laitoksen omistamille tiedostoille	Peruspalvelu. Laitoksella on yhteinen levykiintiö.
Langaton verkko Aalto, Aalto Open ja Eduroam [9] [10]	Peruspalvelu (Aalto open vain Otaniemessä)
Adobe Connect [11]	Henkilökunnalle
Mikroluokat	Peruspalvelu
Virtuaalipalvelimet	Maksullinen (tarkoitettu laitoksille)
Videoneuvotteluhuoneet (H.323) [12]	Peruspalvelu

Taulukko 2 IT-palvelukeskuksen palveluita

2.2 Toivottuja palveluita

Verkon tehokas hyödyntäminen lyhentää välimatkaa kampusten välillä. Apuna voidaan käyttää videoneuvotteluja, videoluentoja ja multicastia. [13] Opiskelijan tai opettajan ei tarvitsisi matkustaa kampukselta toiselle pitääkseen luennon tai päästäkseen luennolle. Luentoja tallentamalla voisi päällekkäisiä luentoja katsoa itselle sopivana aikana. Luentomateriaali on jo nyt siirtynyt lähes kokonaan verkkoon. Verkko-opetus lisääntyy koko ajan.

Nykyaikainen verkko tuo opetukseen aivan uusia mahdollisuuksia. Näiden mahdollisuuksien hyödyntäminen vaatii kurssien [14] järjestäjiltä paljon vaivaa, mutta tekee opiskelusta mielekkäämpää. Luentojen päällekkäisyydet aiheuttavat opiskelijoille ongelmia päivittäin. Tämän ongelmaratkaisun vertailukohtana voi käyttää tallentavaa digiboksia. Moni ihminen on jo tottunut siihen, että omaa suosikkiohjelmaa ei tarvitse katsoa silloin kun se lähetetään, vaan kun sen katsominen sopii. Luentoja voitaisiin lähettää multicastina koko yliopistoverkkoon hyvin edullisesti. Luentojen tallentaminen palvelimelle olisi hyvä palvelu opiskelun tueksi. Luennon mukana näkyisi erillisenä esitykseen liittyvä materiaali.

Yhteisen ajan löytäminen harjoitustyön tekemiseen päiväsaikaan voi olla hankalaa. Tähän auttaa kevyt videoneuvottelupalvelu esimerkiksi Adobe Connect Pro. Opiskelijat voivat käyttää omaa videoneuvottelutyöhuonettaan ja keskustella harjoitustyön yksityiskohdista iltaisin.

Yhteinen aika löytyy klo 21 jälkeen yleensä helpommin. Tähän aikaan yliopiston tilat ovat usein jo suljettuina ja kaikki ovat mielellään jo kotona.

2.3 Erikoisohjelmistot

Opetuksessa tarvitaan koko ajan enemmän erikoisohjelmistoja joita pitäisi kyetä tarjoamaan tutkijoiden, opiskelijoiden ja opettajien käyttöön ympäri vuorokauden. Usein lisenssit ovat kuitenkin niin rajoitettuja, että ohjelmistoja ei voi asentaa omiin koneisiin vaan ainoastaan yliopiston koneille. Opetuksessa käytetään edelleen paljon opetusluokkia, joissa tehdään itsenäisesti ja johdetusti harjoituksia.

Erikoisohjelmistot pyritään hankkimaan yliopistolla kelluvina lisensseinä. Tämän vuoksi nuo sovellukset voidaan asentaa periaatteessa kaikkiin luokkiin. Ainoa huoli on miten saada vapautettua lisenssi tarvittaessa juuri opetustilanteisiin. Lisenssien varaaminen kurssien käyttöön opetuksen ajaksi on vielä vaikeaa. Ainoa keino on katkaista ylläpitäjän tunnuksilla lisenssit kaikilta jotka ovat muualla kuin opetusluokassa.

Esimerkkejä kelluvista lisensseistä, joita ei voi asentaa kotikoneelle:

- Autocad
- Matlab
- Mathematica

3 Verkon perusrakenteet

3.1 Aalto-yliopiston verkon nykytila

Aalto-yliopiston muodostaneiden kolmen korkeakoulun verkot on yhdistetty toisiinsa valopoluilla. [15] Aallon järjestelmät rakennetaan valopolkujen yli kulkevaan verkkoon. Työasemat ja tulostimet ovat kiinni vanhoissa kytkinverkoissa, jotka on liitetty toisiinsa kampusreitittimessä.

Suurin osa kytkinporteista on nopeudeltaan 100 Mbps. Uusissa tietokoneissa on poikkeuksetta 1 Gbps verkkokortti. Normaalissa toimistosovelluskäytössä 100 Mbps ei rajoita vielä mainittavasti käyttömukavuutta. Kaikki tieto siirtyy vähitellen verkkoon tehden työasemasta tai kannettavasta tietokoneesta vain välikappaleen tiedon käsittelyyn. Tämä suuntaus vaatii nopeaa ja luotettavaa verkkoa. [16]

3.2 Verkon suunnittelu

Verkon suunnittelu on kokonaisuuden hallintaa. Verkko ei ole riippumaton ympäröivistä palveluista, vaan ne pitää sovittaa yhteen. Mahdollisimman suuren kustannus- ja suorituskykyhyödyn tavoittamiseksi on mietittävä palvelinten, levyjärjestelmien ja varmuuskopiointien vaatimukset suhteessa verkkoon. Verkon rakenteen perusteella voi olla järkevää käyttää vain IP-pohjaisia (Internet Protocol), esimerkiksi iSCSI [17] (Internet Small Computer System Interface) levyjärjestelmiä. Levyjärjestelmien ja varmuuskopiointien hajauttaminen IP:n yli eri kampuksille toisi varmuutta tiedon säilymiseen ongelmatilanteiden varalle. IP-pohjaisilla [18] tekniikoilla erillisen FC – verkon (Fibre Channel) [19] rakentamiskustannuksilta vältytään. Kustannukset ovat huomattavia etäisyyden kasvaessa.

FC on yleisin tekniikka levyjärjestelmien toteuttamiseen. FC:llä toteutetut tallennusverkot ovat perinteisiä konesaliratkaisuja. Niiden tuki on hyvä ja niiden hallintaa osaavia ylläpitäjiä löytyy paljon. FC:n heikkous on sen tarvitsemat tietoliikenneverkosta riippumattomat valokaapeliyhteydet. Ne nostavat kustannuksia ja korottavat erityisesti pienten organisaatioiden FC:n käyttöönottokynnystä.

Kokonaisuuden suunnittelu korostuu, kun halutaan hajautettu konesalimalli, jossa kaikki palvelut voidaan jakaa vähintään kahteen konesaliin. Luonnostaan tähän malliin taipuvia järjes-

telmiä on vähän. Hitaiden yhteyksien tapauksessa olisi järkevää saada esimerkiksi kotihakemisto-palvelin sen kampuksen konesaliin, jossa henkilö enimmäkseen työskentelee.

Kotihakemistoon pitäisi päästä turvallisesti kaikkialta maailmasta esimerkiksi SSL-suojatun (Secure Sockets Layer) [20] WebDAV:in (Web-based Distributed Authoring and Versioning) yli. Tämä korostuu yliopistomaailmassa, jossa työskennellään monessa paikassa ja erityisesti opiskelijat pääsisivät käsiksi omiin tiedostoihinsa kaikkialta. Tässäkin pitää tasapainoilla tietoturvan ja käytettävyyden kanssa. Käyttäjille pitää saada selkeä käsitys mistä yliopiston järjestelmään voi ja uskaltaa ottaa yhteyttä. Salasanan päätyminen vääriin käsiin on hyvin todennäköistä, jos sen syöttää vieraassa ympäristössä.

3.3 Vaatimukset verkolta ja sen palveluilta

Yliopistoverkon pitäisi siis olla yksinkertainen, nopea, kohtuuhintainen, helppo ylläpitää ja luotettava. Palveluiden pitää toimia hajautettuna vähintään kahteen konesaliin vikasietoisuuden vuoksi. Toipumissuunnitelma pitää löytyä jokaiselle järjestelmälle varavoimakoneista virtuaalipalvelimiin.

Mahdollisuuksien mukaan tietojärjestelmät pitää suunnitella etäkäytettäväksi Internetin yli. Aina ei ole tarpeen, eikä tehokasta työskennellä omassa työpisteessä. Palveluiden pitää toimia vaivattomasti myös seminaari- tai luentomatkalla.

Langattomien verkkojen merkitys kasvaa päivä päivältä. Opiskelijoiden, henkilökunnan ja vieraiden kannettavien tietokoneiden käyttöä pitää tukea tarjoamalla nopeat ja helppokäyttöiset langattomat verkkoyhteydet kaikilla kampuksilla.

3.4 Konesalit, jäähdytys ja varavoima

Konesalit ovat merkittävä osa-alue palveluita suunnitellessa. Nerokkaimmatkin sovellukset vaativat alleen luotettavan ja helppohoitoisen ympäristön. Ympäristö koostuu konesaleista, palvelimista ja tietoliikenneverkosta. Konesalien suunnitteluun on viime vuosina panostettu paljon. Se työ on tuottanut älykkäitä ja energiatehokkaita ratkaisuja. Konesalien sähkökustannukset ja jäähdyttäminen maksavat korttipalvelimen hinnan sen 5 vuoden elinkaaren aikana.

0,1 EUR/kWh x 0,5 kW x 24 tuntia x 365 päivää x 5 vuotta = 2190 EUR.

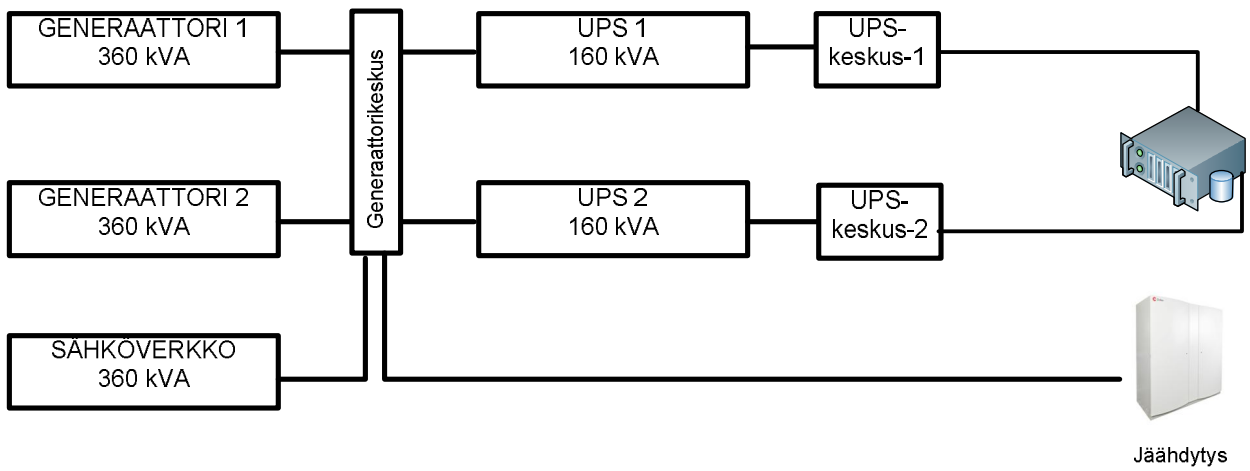
0,5 kW on arvioitu yhteenlaskettu laitteen ja jäähdytyksen tarvitsema teho.

Energiatehokkuutta [21] on parannettu virtualisoimalla palvelimia ja käyttämällä korttipalvelimia siellä missä virtualisointi ei ole mahdollista. Virtualisointi asettaa kovempia vaatimuksia ympäröiville perusjärjestelmille. Tarvitaan nopeampia levyjä, verkkoyhteyksiä ja varmuuskopiointijärjestelmiä. Huomaamatta on tultu tilanteeseen, jossa 50 virtuaalipalvelinta ovat riippuvaisia yhdestä palvelinlaitteesta.

Konesalien pinta-alatehokkuus paranee palvelinten kehittymisen myötä entisestä 20 palvelimesta yli 60 palvelimeen räkissä. Sähkönsyötön ja jäähdytyksen suunnittelulta ja toteutukselta edellytetään aivan uudenlaisia asioita. Sähkönsyöttö pitää rakentaa kahdesta eri UPS-järjestelmästä (Uninterruptible Power Supply). [22] Niille tarvitaan riippumattomat generaattorit. Generaattorit ja UPS:it ovat rinnankäyviä. Sähkönsyöttö konesaliin on turvattu, kun edes toinen generaattoreista on käynnissä.

Generaattorit [23] tahdistuvat verkkoon siten, että on mahdollista käyttää niitä sähköverkon rinnalla. Tarvittaessa voidaan siirtää katkottomasti koko sähkönsyöttö sähköverkolta generaattoreille. Tästä on hyötyä UPSien huoltotilanteessa ja näiden ominaisuuksien testaaminen on tärkeää. Käytännössä syötön siirtyminen pitäisi testata kuukausittain ja testitulokset pitäisi raportoida generaattorien huoltokirjaan.

Generaattorin ja UPSien toiminnan tuntevia ihmisiä tarvitaan useita. Loma-aikanakin pitää aina löytyä joku, joka ymmärtää, miten järjestelmä toimii. Hän pystyy tarvittaessa toimimaan linkkinä generaattorien ja UPS-laitteiden huoltajien kanssa. Kokonaisuuden hallitseminen on välttämätöntä, kun mietitään konesalien perusjärjestelmiä. Huolimattomasti suunniteltu yksityiskohta voi aiheuttaa suurta vahinkoa.



Kuva 1

Kuvassa 1 on pelkistetty kaavio sähkönsyötöstä konesaliin. Sähkönsyöttöjä on kolme. Järjestelmässä on kaksi generaattoria ja valtakunnanverkko. Kaikki kolme syöttöä on suunniteltu rinnankäyviksi. Riittää kun yksi kolmesta syötöstä toimii.

Normaalitilanteessa sähkönsyöttö tulee sähköverkosta ja UPS:ien suojaama kuorma syötetään palvelimille kahden riippumattoman UPS-keskuksen kautta. Näin suojaudutaan UPS-keskuksen tai UPS:ien vioilta ja inhimilliseltä erehdykseltä. Kaikki palvelimet toimivat vielä vaikka toinen UPS:eista ei enää syöttäisi sähköä lainkaan.

Sähköjärjestelmän mitoituksessa on huomioitu jäähdytyksen tarvitsema teho. Jäähdytyslaitteita ei suojata UPS:eilla, vaan ainoastaan generaattoreilla. Sähkökatkon aikana konesalin lämpö voi ilman jäähdytystä nousta hyvin nopeasti. Jäähdytyksen hajauttaminen ja ilmankierto on suunniteltava tarkasti. Näin varmistetaan, että jäähdytyksen yhden osan vikaantuminen ei välittömästi saa aiheuttaa lämpötilan nousua.

Konesaleihin sijoitetaan paljon arvokasta laitteistoa ja tietoa. Järjestelmän jokainen osa pitää suunnitella siten, että siitä ei muodostu yksin vikaantuessaan koko konesalin lamauttavaa ongelmaa. Räkkikaappien sisäinen ilmankierto on hyvä miettiä niin, että hätätilanteessa voi ko-

nesalin ilmaa hyödyntää jäähdytyksessä. Pelkästään räkin sisällä kiertävä ilma lämpenee muutamassa minuutissa.

Jäähdytyksen ohjaus kiinteistöautomaatiossa pitää varmistaa siten, että sitä ei saa sieltä sammutettua lainkaan. Konesalin jäähdytyksen lämpötilaa ja puhaltimien pyörintänopeutta voi säätää, mutta taustalla pitää olla minimitoiminnallisuus, joka huolehtii konesaliin tietyn maksimilämpötilan kaikissa olosuhteissa.

Jäähdytykseen on kehitetty monta tekniikkaa. Esimerkkeinä voi mainita maajäähdytyksen, kaukokylmän, suorajäähdytyksen ja perinteisen kompressorijäähdytyksen. Paras lopputulos saadaan, kun konesalin jäähdytyksessä voidaan käyttää vähintään kahta erilaista, toisistaan riippumatonta tekniikkaa. Tästä syystä pieniä konesaleja ei kannata rakentaa ellei samaa jäähdytystä ja sähköjärjestelyjä voida hyödyntää muihin tarpeisiin.

Konesalien kylmä- ja kuumakäytävät ovat yksinkertainen tapa järkeistää ilmankiertoa. Käytännössä joka toisella käytävällä näkyvät palvelimet edestä ja joka toisella takaa. Tämä helpottaa jäähdytyksen suunnittelua. Kylmä ilma johdetaan sinne mistä palvelimet sen luonnostaan imevät. Lämmin ilma menee poistokanaviin, jotka ovat kuuman käytävän kohdalla.

4 Palvelimet

4.1 Lähtötilanne

Palvelinten asentaminen ja valvonta on aikaisemmin hoidettu kirjavasti. Korkeakoulusta ja käyttöjärjestelmästä riippuen työ on ollut enemmän tai vähemmän käsityötä. Valvontajärjestelmiä on ollut useita ja niiden välillä ei ole ollut mitään yhteyttä. Erilaisia hälytyksiä on tulkittu sähköposteista ja kuvaajista.

Asennusten dokumentointi on jäänyt usein asentajan muistin ja tahdon varaan. Yhtenäisiä tapoja asennusten tekemiseen ei ole ollut. Käytännössä suuri osa asetuksista on jouduttu tekemään käsin käyttöjärjestelmäasennuksen jälkeen. Ohjeet tuleville, saman asennuksen mahdollisti uudestaan tekeville ihmisille, ovat tekstitiedostoja ja skriptejä.

Hankitut palvelimet ovat pahimmillaan olleet joka tilauskerralla erilaisia. Vakiointia ei ole kunnolla ymmärretty, vaan kolme perättäistä laitehankintaa ovat saattaneet päätyä eri laitevalmistajien toimitettaviksi. Tämä ei mitenkään edistä ylläpitäjien osaamista laitteista, vaan aiheuttaa ylimääräistä selvitystyötä laitteiden ja ohjelmistojen osalta.

Varaosien, laajennusten tai lisäosien tilaaminen voi olla ylläpitäjille työlästä, jollei hän ei ehdi kunnolla tutustua yhden valmistajan tuotteisiin. Oman henkilökunnan tekemä työ näiden asioiden selvittämiseksi voi olla huomattavan kallista. Huoltokutsujen, varaosien ja päivitysten kannalta palvelinten vakionti on tärkeää.

4.2 Palvelinten asentaminen ja valvonta

Palvelinten asentaminen ja valvonta pitää automatisoida. Palvelimen käyttöjärjestelmän ja päivitysten asentamiseen ei saa kulua tuntia enempää aikaa ja se on pystyttävä tarvittaessa tekemään kymmenille koneille yhtä aikaa. Palvelinhallinnan ylläpidon jakaminen koko yliopiston laajuisesti on tärkeää. Näihin ylläpitojärjestelmiin panostetaan paljon rahaa ja aikaa.

Samaa työtä ylläpitojärjestelmien kehittämiseksi ei voida tehdä kaikissa laitoksissa uudestaan, vaan keskitetyn järjestelmän pitää olla delegoitavissa. Laitoksen ylläpitäjä näkee vain oman

laitoksen palvelimet ja voi niihin kohdistaa keskitetysti tehtyjä valmiita tehtäviä. Näin saadaan keskittämisen edut ja rajataan ylläpito-oikeudet oikeisiin palvelimiin.

Sovellusten asentamisen automatisointi on järkevää jos sama asennus toistuu usein. Yksittäisten asennusten automatisoinnin voi toteuttaa levykuvalla, jolloin tiettyyn tilanteeseen pääsee tarvittaessa hyvin nopeasti. Levykuvien haaste on ollut käyttöjärjestelmien rautariippuvuus. Tämä on kehittynyt viime vuosien aikana parempaan suuntaan. Edelleen voi kuitenkin törmätä ongelmaan, jossa levykuvaa ei voi palauttaa erilaiseen palvelimeen.

Yksilölliset muutokset levykuvan palauttamisen jälkeen onnistuvat skripteillä tai hallintajärjestelmän tekniikoilla. Muutostenhallinnan ja palautteen saamisen kannalta hallintajärjestelmän tekniikat ovat järkevämpi valinta. Tapahtumien kulkua voidaan jälkeenpäin valvoa ja ongelmatilanteissa vian selvittäminen helpottuu merkittävästi. Hallintajärjestelmien käyttöönotto vaatii paljon aikaa ja niistä saatava hyöty varmistuu vasta kun työntekijät osaavat ja tuntevat järjestelmän hyvin. Pienessä ympäristössä järjestelmän edut eivät pääse oikeuksiinsa. Palvelinten määrän ylittäessä 50 muuttuu hallintajärjestelmä jo välttämättömyydeksi.

4.3 Palvelinten levyjärjestelmä

Keskittämällä palvelinten levyt levyjärjestelmään (storage area network = SAN) voi palvelinten levynkulutusta hallita joustavasti ja käytettävien levyjen määrää vähentää. SAN-järjestelmät eivät välttämättä tuo kustannussäästöjä, mutta niiden avulla kokonaisuus on hallitumpi. Suurissa konesaliympäristöissä myös palvelinten käyttöjärjestelmälevyt tulevat levyjärjestelmästä. Tätä kutsutaan boot from SAN:iksi. [24]

Boot from SAN:in vahvuutena on palvelinlaitteen ja tiedon eristäminen toisistaan. Konesali voi sijaita satojen kilometrien päässä ja silti ylläpitäjä voi vaihtaa palvelimen levyn toiseen palvelimeen hyvin nopeasti. Tämä on hyödyllistä silloin kun palvelinlaite vikaantuu. Käyttöjärjestelmän levyalueet siirretään varapalvelimelle ja palvelu käynnistetään uudella laitteella.

4.4 Palvelinten varmuuskopiointi

Varmuuskopioinnin luonne on muuttunut tallennettavan tiedon määrän kasvaessa jatkuvasti kiihtyvään tahtiin. Perinteistä varmuuskopiointia tehdään enää vain tärkeälle tiedolle. Vähemmän arvokas tieto kopioidaan yhteen tai useampaan paikkaan eikä sitä välttämättä erikseen enää arkistoida nauhoille tai vastaaville perinteisille varmuuskopiointijärjestelmille. Tiedon kasvava määrä pakottaa luokittelemaan ja miettimään mitä todella pitää säilyttää. Tämä luokittelu pitäisi tehdä tiedon tallentamisvaiheessa. Jälkeenpäin se on huomattavasti vaikeampaa ja työläämpää.

Varmuuskopiointia joudutaan hajauttamaan usealle varmuuskopiointipalvelimelle valtavien tietomäärien takia. Varmuuskopiointinauhureita voi olla kymmeniä. Näin voidaan varmistaa useita kymmeniä palvelimia yhtä aikaa ja tarvittaessa myös palauttaa tiedostoja keskeyttämättä varmuuskopiointeja. Kehittyneet snapshot – tekniikat levyjärjestelmissä mahdollistavat tuotantotietokantojen varmuuskopioinnin niiden käytön aikana. Tilanne vastaa varmuuskopioitavaa palvelinta sammutettuna. Tällainen ei ole perinteisellä palvelimella mahdollista vaan aina joudutaan tyytymään erilaisten agenttien tekemiin varmuuskopiointeihin.

5 Työasemat

5.1 Työasemien nykytila

Työasemien ja kannettavien tietokoneiden tilanne Aalto-yliopistossa ei ole hyvä. Laitoksien sisällä on omia atk-keskuksia ja pahimmillaan tutkijat käyttävät omilla rahoilla ostamiaan tietokoneita ja laittomia lisenssejä. Laboratorioiden yhdistyttyä laitoksiksi voi vielä olla jäljellä neljä eri järjestelmää laitoksen sisällä.

Hajaantuneisuus tarkoittaa väistämättä tyhjäkäyntiä ja vääriä hankintoja. Aikaa kuluu tietokoneiden vertailuun ja kaupoissa kiertämiseen. Laitteiden takuut ovat kirjavia ja niiden huoltokäytännöt eivät ole kenenkään tiedossa. Takuun ja huollon merkitys korostuu kannettavissa tietokoneissa. Käyttäjä voi pahimmillaan joutua odottamaan kaksi viikkoa koneen huoltoa ja kuljettamaan sen itse.

Koneiden rahoitus on hoidettu laitoksittain kirjavasti. Yhdessä laitoksessa koneet ostetaan tutkimusryhmittäin eri rahoista. Toisessa laitoksessa koneet sentään ostetaan laitoksen yhteisellä rahalla eli silloin resurssit käytetään vähän tehokkaammin. Projektin päättymisen jälkeen koneet voidaan antaa seuraavalle työntekijälle, vaikka hän ei kuuluisikaan samaan tutkimusryhmään.

5.2 Työasemien hankinta

Työasemien luonne muuttuu työelämän mukana yhä liikkuvammaksi. Aalto-yliopistossa yhden tietokoneen periaatetta noudatetaan jo luonnostaan. Kannettavien tietokoneiden määrä lisääntyy koko ajan sekä henkilökunnalla, että opiskelijoilla. Samalla henkilökunnan kannettavista tietokoneista pyritään tekemään vain työkaluja, eikä yksittäisiä yksilöllisiä virityksiä sallita. Tämä toteutuu kun kannettavien asennus ohjelmistoineen tapahtuu nopeasti ja vakioidusti. Hankinta on keskitetty ja valikoima on riittävä. Jokainen työntekijä löytää itselleen sopivan koneen yliopiston tuettujen koneiden valikoimasta.

Keskitetyillä laitehankinnoilla on paljon etuja. Toimittajat pystyvät ennakoimaan laitetarpeita ja toimitukset nopeutuvat viikoista tunteihin. Koneita ei hyvän asennusjärjestelmän ansiosta

tarvitse kuljettaa ensin asennettavaksi johonkin IT palveluiden pisteeseen, vaan kaikki käyttöjärjestelmästä ohjelmistoihin asennetaan automaattisesti työpisteellä. Tämä järjestelmä helpottaa toipumista kovalevyn hajoamisesta tai koneen vaihdosta.

Uusi kone voidaan toimittaa suoraan työntekijän työpöydälle ja vanha viedään samalla takaisin yliopiston varusvarastolle jossa se kierrätetään ja kaikki yliopiston omistama tieto poistetaan kovalevyn tyhjennysohjelmistolla. Kiireellisissä tapauksissa työntekijä voi mennä suoraan varusvarastolle ja saada korvaavan koneen heti käyttöönsä. Samalla tavalla toimitettaisiin uusi akku, verkkokaapeli tai matkalaturi.

5.3 Toimituksien oikea-aikaisuus ja tehokkuus

Yliopiston kannalta on tehokkaampaa keskittyä työn tekemisen helpottamiseen toimittamalla välttämättömät työkalut nopeasti. Väärinkäytöksien estämiseksi kaikki kirjataan ja jokaisen työntekijän kohdalla eritellään täydellinen historia työvälineistä. Historia sisältäisi kaikki varusvarastolta kuitatut tavarat. Kaikki myös palautetaan varusvarastolle työsuhteen päättyessä. Tämä poistaisi tyhjäkäyntiä projektien rahoilla hankittujen tietokoneiden ja tarvikkeiden makuuttamisesta tyhjissä työhuoneissa odottamassa seuraavaa projektia.

Varusvaraston rahoitukseen ehdotetaan yleensä keskusteluissa sisäistä laskutusta. Selkeä ja yksinkertainen tapa on vakioida mallit siten, että kustannukset ovat hyvin lähellä toisiaan laitevalinnoista riippumatta. Työvälineiden nopea toimitus on tärkeää, mutta vielä tärkeämpää on mitä niillä välineillä työntekijä saa aikaan. Kustannukset on järkevää hoitaa keskushallinnon yleiskustannuksista. Tästä on saatu hyviä kokemuksia kalusteiden ja matkapuhelinten hankinnassa ja puhelinlaskujen keskittämisessä.

Ohjelmistojen hankinnassa saadaan säästöjä, kun ohjelmistot hankitaan keskitetysti ja mahdollisuuksien mukaan kelluvina lisensseinä. Myös sovellusvalikoimaa voidaan ohjata kun ne hankitaan todellisen tarpeen mukaan. Apuvälineenä voidaan käyttää hallintajärjestelmien raportointityökaluja. Niiden avulla näkee suoraan onko jotain ohjelmaa käytetty lisenssimäärää vastaavalla tavalla. Erikoisohjelmistoja tulee aina olemaan, mutta hoitamalla yleiset ohjelmat helposti kaikille voi laitosten henkilökunta keskittyä oman alansa erikoisohjelmiin. Tottumukset ohjaavat usein ohjelmistovalintoja ja näissä on tärkeää saada tunnekysymyksien vastineeksi moninkertainen määrä järkiperusteita.

5.4 Työasemien verkot

Langattomien verkkojen käyttö lisääntyy jatkuvasti ja niiden laatu ja turvallisuus hallituissa ympäristössä on parantunut huomattavasti. Suojaamalla radiotien yli kulkeva liikenne kuuntelulta voidaan avata pääsy suoraan langattomasta verkosta verkkolevyille ja vastaaviin palveluihin. Käyttäjän kannalta on tärkeää, että jokaista käyttötilannetta varten ei tarvitse toimia eri tavalla.

Työasemaympäristön palvelut voidaan suunnitella niin, että niitä on turvallista käyttää suoraan Internetistä. Tämä edellyttää hyvin yksinkertaista ja homogeenista ympäristöä, jollaista ei yliopistoverkoista helposti saa. Useat tuetut käyttöjärjestelmät kuten Windows, Linux ja Mac tekevät palveluiden toteuttamisesta vaikeampaa. Jokaisella käyttöjärjestelmällä on erilainen luontainen tapa toimia. Käyttöjärjestelmiä yhdistettäessä yhdeksi palveluksi joudutaan väistämättä tekemään kompromisseja. Kotihakemistojen toteuttaminen turvallisesti tai tulostaminen käyttäen käyttäjätunnusta ja salasanaa eivät ole helppoja toteuttaa.

Tunnettuihin ja turvallisina pidettyihin verkkoihin on helppo avata näitä palveluita. Verkko voidaan tunnistaa julkisen avaimen tekniikkaan perustuvalla suojausmekanismilla esimerkkinä porttiautentikointi 802.1X. [25] Siinä kone tai käyttäjä tunnistetaan ja sen perusteella rasiasta tuleva verkko kytketään tiettyyn aliverkkoon automaattisesti. Vieraiden koneille, eli niille jotka eivät kykene tunnistautumaan, kytketään automaattisesti vierailijaverkko. Koneita voidaan tunnistaa myös verkkokortin fyysisen osoitteen perusteella, mutta sitä ei voi pitää kovin luotettavana tai turvallisena tapana. Tuon osoitteen voi vaihtaa helposti.

802.1X:ää voidaan käyttää myös langattomissa verkoissa. Aalto-yliopiston langattomassa verkossa voitaisiin käyttää enterprise WPA2 – suojausta (Wi-Fi Protected Access version 2). [26] Sen avulla kaikki keskitetysti ylläpidetyt kannettavat työasemat pääsisivät suoraan kiinni tunnistautumis- ja levypalveluihin myös langattomasti.

Käyttäjien liikkuvuuden takia verkkojen käyttö pitää tehdä mahdollisimman joustavaksi ja helpoksi. IP-asetusten jakaminen automaattisesti DHCP:llä helpottaa koneiden käyttöönottoa ja se tarvitaan poikkeuksetta myös hallinta- ja asennusjärjestelmien kanssa.

Automaattinen koneiden aliverkkojen hallinta on jo paljon harvinaisempaa. Sen esteenä ovat usein puutteelliset järjestelmät, hajaantunut ylläpito ja vanhat verkkolaitteet. 802.1X:n käyttöönotto vaatii usean osapuolen yhteistyötä. Työasemille tarvitaan varmenteet niiden tunnis-

tamista varten. Verkkolaitteiden pitää saada yhteys käyttäjätunnuspalveluun (RADIUS), jos vain käyttäjä tunnistetaan.

5.5 Työasemaverkon suorituskykytarve

Työasemien verkkojen nopeustarve kasvaa jatkuvasti. Koneiden paikallisella levyllä ei saa olla käyttäjän tekemiä tiedostoja, vaan ne pitää säilyttää verkkolevyllä. Syy tähän on käyttäjien siirtyminen koneelta toiselle ja käyttäjän tiedostojen suojaaminen kovalevyn hajoamisen varalle. Kannettavissa tietokoneissa voidaan osa verkkolevyllä olevista hakemistoista kopioida paikalliselle kovalevylle käyttöjärjestelmien automaattisilla menetelmillä. Samat menetelmät huolehtivat myös tiedostojen synkronoinnista takaisin verkkolevylle verkkoyhteyden palautumisen jälkeen. Näin tiedostoja voidaan käyttää myös verkkoyhteyttä. Verkkolevyjen synkronointi vaatii huolellisuutta. Joku muu on voinut ehtiä muuttaa tiedostoja sillä aikaa kun, ne ovat olleet toisen käyttäjän mukana ulkomaanmatkalla. Tässä tilanteessa synkronointia tekevälle käyttäjälle näytetään ehdotus toisen kopion tekemisestä. Sillä vältetään muutoksien häviäminen.

5.6 Työasemapalvelut liikkuville käyttäjille

VPN-yhteyksien (Virtual Private Network) käyttäminen on helppoa. VPN-yhteys voidaan avata vierailijaverkosta tai vaikka kotoa ADSL:n takaa. VPN tuo yliopiston verkon tietokoneelle toisen yhteyden yli. VPN:n tunnistamisessa voidaan käyttää samoja varmenteita joita hyödynnettäisiin porttiautentikoinnissa 802.1X. Tavallinen VPN yhteys on L2TP -suojattuna IPSecillä. L2TP on tunnelointiprotokolla ja IPSec salaa liikenteen ulkopuolisilta. VPN-yhteyden avaamisen jälkeen tietokone toimii kuin se olisi yliopiston verkossa. VPN-yhteys tuo mukanaan ylimääräisen kerroksen verkkoliikenteeseen, eikä sen yli toimi vaivattomasti kaikki verkon palvelut.

6 Käyttäjätunnukset ja käyttöoikeudet

6.1 Käyttäjähallinnon lähtötilanne

Kolmen korkeakoulun lupahallintojärjestelmät ovat täysin erilaisia ja kaikkiin liittyy käsityötä. Tunnuksia haetaan erikseen ja niiden tietoja syötetään käsin. Käyttäjätunnusten tekemiseen ja hallinnointiin kuluu useita henkilötyövuosia ja vääriä tunnuksia on avoinna unohduksien takia.

Unohtuneen salasanan vaihtoon ei ollut korkeakouluilla itsepalveluvaihtoehtoa, vaan aina oli mentävä asiakaspalveluun. Uusien opiskelijoiden tunnuksien luonti ja jako ovat erityisesti Otaniemen kampuksella olleet jokavuotinen voimainkoitos.

Erilaisia järjestelmiä on kytketty lupajärjestelmiin jakelemalla perinteisiä salasana-tiedostoja unix-järjestelmiin, LDAP-hakemiston [27] avulla Linuxeille ja Active Directoryyn Windows-koneille. Salasanan vaihdon jälkeen uusi salasana tulee vasta tunnin sisällä voimaan, mikä voi opetustilanteessa olla liian pitkä aika.

TKK:lla käyttäjällä on käytössään 4 eri salasanaa samaan käyttäjätunnukseen. Niitä ovat pääsalasana, palvelusalasana, verkkosalasana ja sähköpostisalasana. Tästä käyttäjät eivät ymmärrettävästi ole pitäneet. Salasanojen määrä on lähtöisin tietoturvan vaatimuksista. Käytännössä on huomattu, että tietoturva paremminkin heikkenee kun salasanojen määrä kasvaa. Kun samalla salasanalla pääsee kaikkiin palveluihin käyttäjä muistaa sen eikä kohtele sitä välinpitämättömästi.

6.2 Käyttäjätunnusten automatisointi

Yliopistoissa henkilökunta vaihtuu nopeasti ja tunnuksia on paljon. Aalto-yliopistossa käyttäjätunnuksia on yli 30000. Tunnusten hallinta käsin ei ole järkevää, vaan niiden elinkaari hoidetaan rekisterien perusteella. Henkilökunnan tunnukset tehdään henkilöstöhallinnon tietojen perusteella. Kerran vuorokaudessa työntekijöiden tiedot välitetään lupahallintoon. Työsuhteen päättymispäivä merkitään automaattisesti tunnuksen päättymispäiväksi. Työntekijällä voi olla useita työsopimuksia ja niistä pisimpään jatkuva vaikuttaa voimassaoloon.

Vastaavalla tavalla opiskelijoiden tunnukset perustuvat opintotietojärjestelmään. Opinto-oikeus tuo automaattisesti käyttäjätunnuksen. Opiskelijalla voi olla useita opinto-oikeuksia ja ne näkyvät tunnuksen ominaisuuksissa ja ryhmäjäsenyyksissä.

6.3 Käyttäjähallinnan itsepalvelu

Käyttäjätunnusten hakeminen, tekeminen ja poistaminen ovat olleet aikaisemmin hyvin työläitä kaikille osapuolille. Itsepalveluna ei ole ollut mahdollista uusia salasanaa vaan se on ollut ainoastaan mahdollista käymällä asiakaspalvelussa.

Aalto-yliopiston käyttäjätunnukset otetaan käyttöön poliisin myöntämällä sirullisella henkilökortilla tai pankkitunnuksilla. Samalla tavalla salasanan voi vaihtaa jos on unohtanut sen. Halutessaan voi myös asioida asiakaspalvelussa, mutta se ei ole enää pakollista.

6.4 Kertakirjautuminen

Kertakirjautuminen eri järjestelmien välillä vähentää käyttäjien ärtymystä sekä tietoturvaongelmia. Työasemaan kirjautumisen jälkeen ei käyttäjältä pitäisi kysyä samaa salasanaa enää uudestaan. Salasanaa voidaan kysyä joissain hyväksyntää vaativissa talousasioissa, mutta silloinkin sen hyödyllisyyttä pitäisi arvioida kriittisesti. Tärkeää olisi, että tällaiset hyväksynnät on helppo tarkistaa ja raportoida jälkeenpäin.

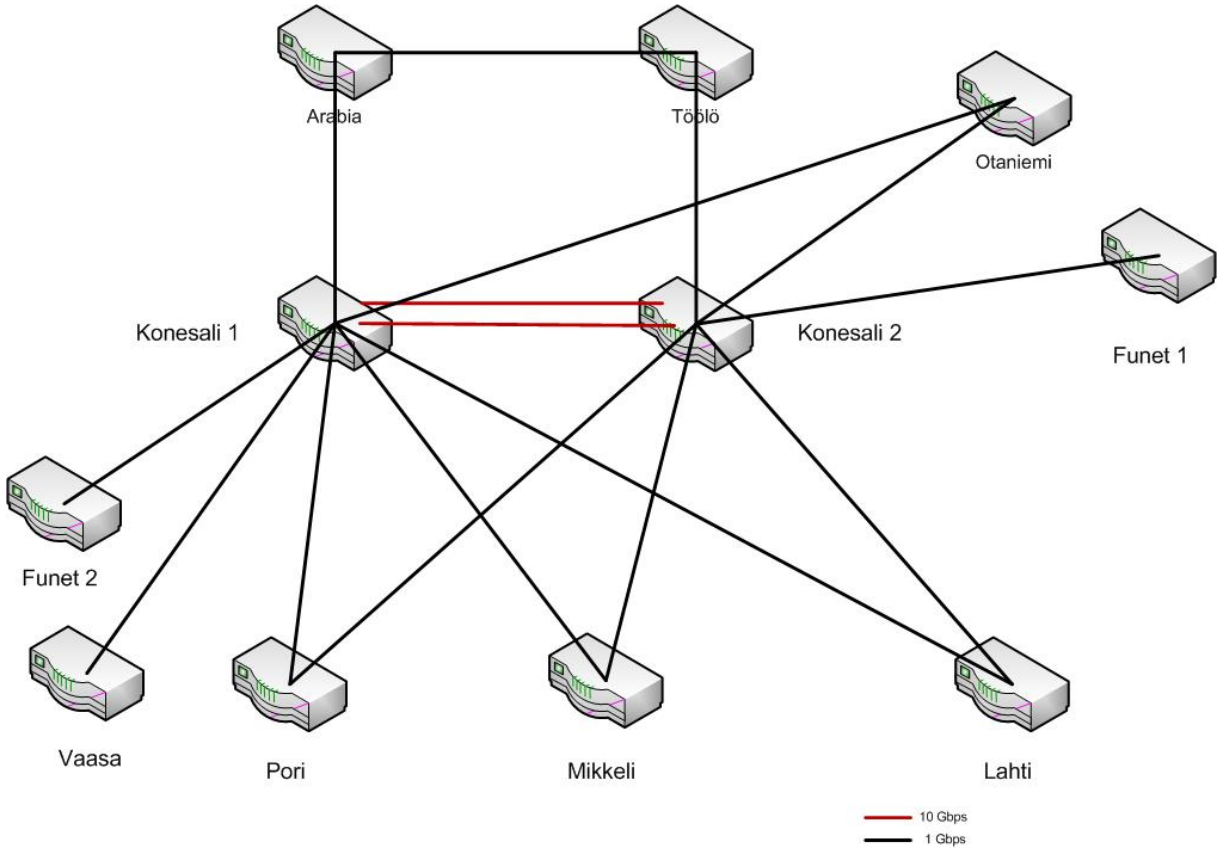
6.5 Ylläpitäjien tunnukset

Käyttäjätunnuksia tehdään automaattisesti myös ylläpitotarkoitukseen. Työntekijän nimikkeen perusteella tehdään oletus siitä tarvitseeko hän työasemaylläpitotunnuksia vai lisäksi myös palvelinylläpitotunnuksia. Näitä tunnuksia liitetään laitosten johtajien hyväksynnällä oikeisiin ryhmiin, jonka jälkeen varsinaiset ylläpito-oikeudet tulevat voimaan.

Ylläpitotunnukset liitetään käyttäjätunnukseen ja niillä on sama elinkaari. Ylläpitotunnukselta voidaan ottaa kokonaan erioikeudet pois tai tarvittaessa jopa estää käyttö kokonaan jos se tuntuu tarpeelliselta.

7 Nykyinen Arkkitehtuuri

7.1 Käytössä olevan verkon rakenne



Kuva 2 Käytössä olevan verkon rakenne

Yliopiston Internet-yhteydet tulevat konesaleihin 1 ja 2. Niissä on myös reitittimet, joista kaikki liikenne lähtee yliopistosta ulospäin. Konesalien reitittimiin on suoraan kytkettynä Otaniemen kampuksen kytkinverkkoa ja valopolkujen takana olevat etäkampukset.

Etäkampusten yhteydet ovat reititettyjä. Jokainen linkki on neljän IP-osoitteen aliverkko, jonka taakse on määritelty etäkampuksen aliverkot. Toisella valopolulla on samanlainen staattisilla reiteillä määritetty vaihtoehtoinen reitti etäkampuksen aliverkoille.

Etäkampuksien linkeissä ei käytetä VLAN:eja (Virtual LAN), vaan kaikki liikenne reititetään. Tämä on suojautumista Broadcast-myrskyihin tai vastaaviin L2 -tason verkon ongelmiin. Etäkampuksen sisäiset palvelut toimivat nopeasti ja riippumattomasti kampuksien yhteyksistä.

Tämän ominaisuuden merkitys korostuu käytettäessä esimerkiksi etäkampuksen omaa levypalvelinta tai tulostuspalvelinta.

Kyse on tasapainoilusta palveluiden hajauttamisen ja keskittämisen välillä. Kuinka luotettavia valopolut ovat? Kuinka paljon ylimääräisiä kustannuksia palveluiden hajauttamisesta syntyy? Käyttäjien liikkuessa kampukselta toiselle on pystyttävä avaamaan pääsy etäkampuksen tiedostopalvelimeen toisen etäkampuksen työasemaverkosta. Näitä vaatimuksia on pitkä lista ja päätöksenteon tueksi tarvitaan kustannus- ja luotettavuusarvioita.

7.2 Käytössä olevan verkon toiminnan periaatteet

Etäkampuksien reitittiminä on yksi laite. Tähän reitittimeen on määritetty Aalto-yliopiston työasemapolitiikan mukaiset aliverkot. Työasemaverkkojen välillä ei liikennettä juurikaan ole, vaan kaikki liikenne kohdistuu palvelinverkkoihin ja Internetiin.

Työasemien IP-osoitteet jaetaan automaattisesti käyttäen DHCP:tä (Dynamic Host Configuration Protocol). IP-osoite voidaan tarvittaessa asettaa kiinteäksi DHCP-varauksella. Kirjautumista varten etäkampuksilla on oma palvelin, jonka tehtävänä on varmistaa kirjautuminen työasemiin verkkoyhteyksien ollessa täysin poikki konesaleihin 1 ja 2. Lisäksi palvelinverkossa voi olla esimerkiksi paikallinen tulostuspalvelin ja tiedostopalvelin.

Työaseman käynnistyessä se pyytää verkosta DHCP:llä IP-osoitteen. Se pyyntö välitetään etäkampuksen reitittimestä keskitettyyn DHCP-palveluun. Sieltä aliverkon määrityksien mukaan työasema saa IP-asetukset. Asetuksien perusteella kone voi käyttää verkon palveluita joko yliopiston koneena tai vierailijana.

7.3 Nykyratkaisun edut ja rajoitukset

Reitittäminen etäkampuksilla tuo selvän rajan kampuksien välille. Etäkampuksen sisäiset palvelut ja muilta kampuksilta tulevat palvelut ovat omissa lokeroissaan. Pääsy palveluihin voidaan rajata perinteisesti IP-osoiteavaruuden perusteella. Kampuksien välinen liikenne on pelkästään IP-pohjaista ja kaikki L2-tason häiriöt rajautuvat automaattisesti pois. Paikallisille palveluille saadaan hyvin lyhyt viive ja ne toimivat kunhan vain etäkampuksen reititin toimii.

Reititys on suoraviivainen toteuttaa ja yhteyksien toimimiseen riittää kun toinen linkeistä on kunnossa. Kaikki etäkampuksen ulkopuolinen liikenne ohjataan oletusreittiä ulos ja sen reititys hoidetaan jossain muualla.

Saman VLAN:in käyttäminen eri kampuksilla ei onnistu. Toisinaan tutkimusryhmät voivat olla hajautuneena useammalle kampukselle ja silloin maantieteellinen sijainti vaikuttaa verkkovalintoihin. VLAN:eja levittäessä myös IP-osoitteiden käyttö tehostuu. Samaa käyttötarkoitusta varten ei tarvitse tehdä uutta verkkoa joka kampukselle.

VLAN:eja käytetään joustavasti eri käyttötarkoituksiin. Niiden rajaaminen maantieteellisen sijainnin perusteella vaikeuttaa erityisesti 802.1X porttiautentikoinnin käyttöä. Kannettavan tietokoneen VLAN:in määrittely onnistuu sen avulla automaattisesti koneen saaman varmenteen perusteella. 802.1X:ää käsitellään tarkemmin seuraavissa luvuissa.

VLAN:eja tarvitaan myös IP-pohjaisten levyjärjestelmien levittämiseen etäkampuksille. Nykyisin käytössä olevat iSCSI-levyjärjestelmät on suunniteltu toimimaan samassa VLAN:issa eikä niiden liikennettä ohjeiden mukaan saa reitittää. Levyjärjestelmien toiminta etäkampuksille VLAN:in sisällä riippuu lähinnä vain viiveestä. Viiveen kasvaminen on levyjärjestelmälle suuri ongelma ja se näkyy suoraan sovelluksissa.

Etäkampuksille meneviä linkkejä ei voi hyödyntää kuormantasauksessa, vaan vain toista linkkiä käytetään aktiivisesti ja toinen odottaa mahdollista ongelmatilannetta. Tämä on laadukkaiden ja arvokkaiden valopolkujen vajaakäyttöä. Todellisia kuormahuippuja on vielä harvoin, mutta niiden ilmaantuessa linkkien kuormanjako auttaisi merkittävästi.

Pääsylistojen ylläpito vaatii paljon suunnittelua ja dokumentointia. Yhteyksiä pitää pystyä avaamaan työasemaverkoista kaikkiin palvelinverkkoihin. Käyttäjien liikkuessa kampukselta toiselle on jokaisen palvelinverkon oltava auki kaikkiin työasemaverkkoihin, joista voi mahdollisesti tulla yhteydenottoja.

Palveluiden keskittäminen vie perustelut perinteiseltä L3-verkolta. Käyttäjän näkökulmasta tärkeintä on luotettava, nopea ja joustava verkkoyhteys. Pelkät L3-yhteydet eivät enää riitä, vaan yhteyksien muodostaminen L2-tasolla on välttämätöntä.

1 GE-verkkoyhteydet pääkampuksille Otaniemi, Töölö ja Arabia asettavat rajat verkon käytölle. Kaikki liikenne kulkee samaa 1 GE-linkkiä pitkin. Sen nopeus ei käytön lisääntyessä ole

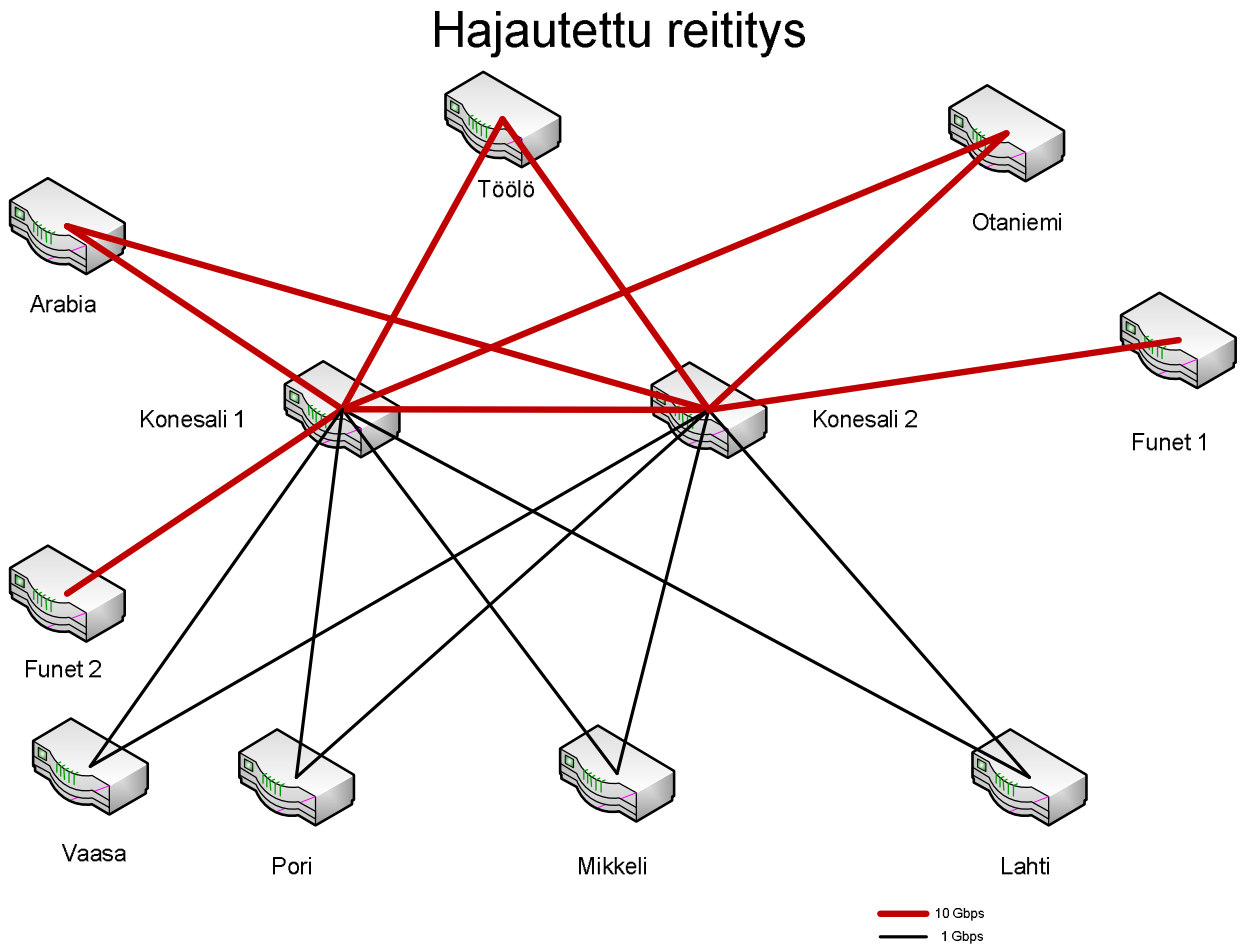
riittävä. Viiden työaseman asennus ja samaan aikaan viiden koneen levykuvan kopiointi toiseen suuntaa riittää täyttämään yhteyden.

Tällä hetkellä on valopolku Arabian ja Töölön välillä. Sillä ei ole paljoa liikennettä, koska Aallon palvelut ovat enimmäkseen konesaleissa 1 ja 2. Linkin hyödyntämisen näkymät ovat nykyratkaisulla aika huonot ja kuormantasauksen kannalta suorastaan vaikeat. Varayhteytenä sitä voi käyttää vain kun pääasiallisen yhteyden linkki on alhaalla. Kaikki liikenne Töölön ja Arabian välillä toki kulkee siinä.

8 Arkkitehtuurivaihtoehto 1 - Hajautettu reititys ja MPLS

8.1 Hajauttamisen periaatteita

Hajauttamalla reititys voidaan kampuskohtaisesti tarjota tiettyjä palveluita vaikka verkkoyhteys olisi poikki molempiin konesaleihin. Tulostus ja tiedostopalvelut ovat tyypillisesti niitä joita ilman on vaikea työskennellä. Hajautettu reititys edellyttää verkon ylläpidolta ammattitaitoa ja järkevästi toteutettuna nykyaikaisten reitityksprotokollien käyttöä.



Kuva 3 Hajautettu reititys

8.2 Reitittimien kytkennät

Etäkampusten reitittimet kytketään konesaleissa oleviin runkoreitittimiin molempiin yhdellä kuituparilla. Yhteydet ovat pääasiassa valopolkuyhteyksiä Funetin [28] kautta. Vaasaan on vain yksi yhteys. Molemmista konesaleista lähtee Internet-yhteys Funetiin. Erityisesti suurempiin kampuksiin tarvittaisiin 10 GE-yhteydet. Yhteyksien pitäisi kulkea eri reittiä. Se vähentää kaivutöiden aiheuttamien linkkivikojen riskiä. Usein vika voi johtua myös inhimillisestä virheestä kytkentätiloissa. Asentaja voi purkaa väärän linjan vahingossa. Vaikka hän huomaa ja korjaa virheen, liitin voi jäädä huonosti kiinni eikä yhteys toimi.

Verkon kaikki reitittimet määritellään käyttämään MPLS:ää (Multiprotocol Label Switching) [29] RSVP:llä (Resource Reservation Protocol) signaloituna. RSVP huolehtii, että LSP (Label Switched Path) avataan kahden reitittimen välillä. Vaikka LSP luodaan automaattisesti, voidaan sen avaama polku suojata ja varmistaa linkkisuojauksella (Link Protection). Sen avulla yhteys siirtyy toiselle reitille nopeasti.

Alun perin MPLS suunniteltiin nopeuttamaan reititystä, mutta reitittimien nopeutuessa alkuperäinen tarkoitus menetti merkityksensä. MPLS:ää hyödynnetään nykyään luomaan uusi kerros operaattoriverkkoon. Sen avulla asiakkaat voidaan eristää verkon sisällä omaan ulottuvuuteensa. TE (Traffic Engineering) tekee mahdolliseksi liikenneluokkien ja prioriteettien määrittelyn. TE:n keinoin voidaan varmistaa määritellyn ja tärkeänä pidetyn liikenteen kulku kaikissa olosuhteissa. Vaihtoehtoisesti sillä voidaan rajoittaa yhteyksien nopeutta palvelusopimuksien mukaiseksi.

Tämä tekniikka antaa mahdollisuuden erilaisten verkkojen ulottamisen kampukselta toiselle reititetyn verkon yli. L2VPN eri kampuksien välillä on helppo toteuttaa reititetyn verkon yli vain käyttäen MPLS:ää. L3VPN:ää käytetään kun yhteyksiin riittää pelkkä IP-tason yhteys. VPLS:n (Virtual Private LAN Service) [30] keinoin voidaan luoda L2VPN:iä dynaamisesti ja se soveltuu suuriin toteutuksiin, joissa määritykset halutaan toteuttaa dynaamisesti.

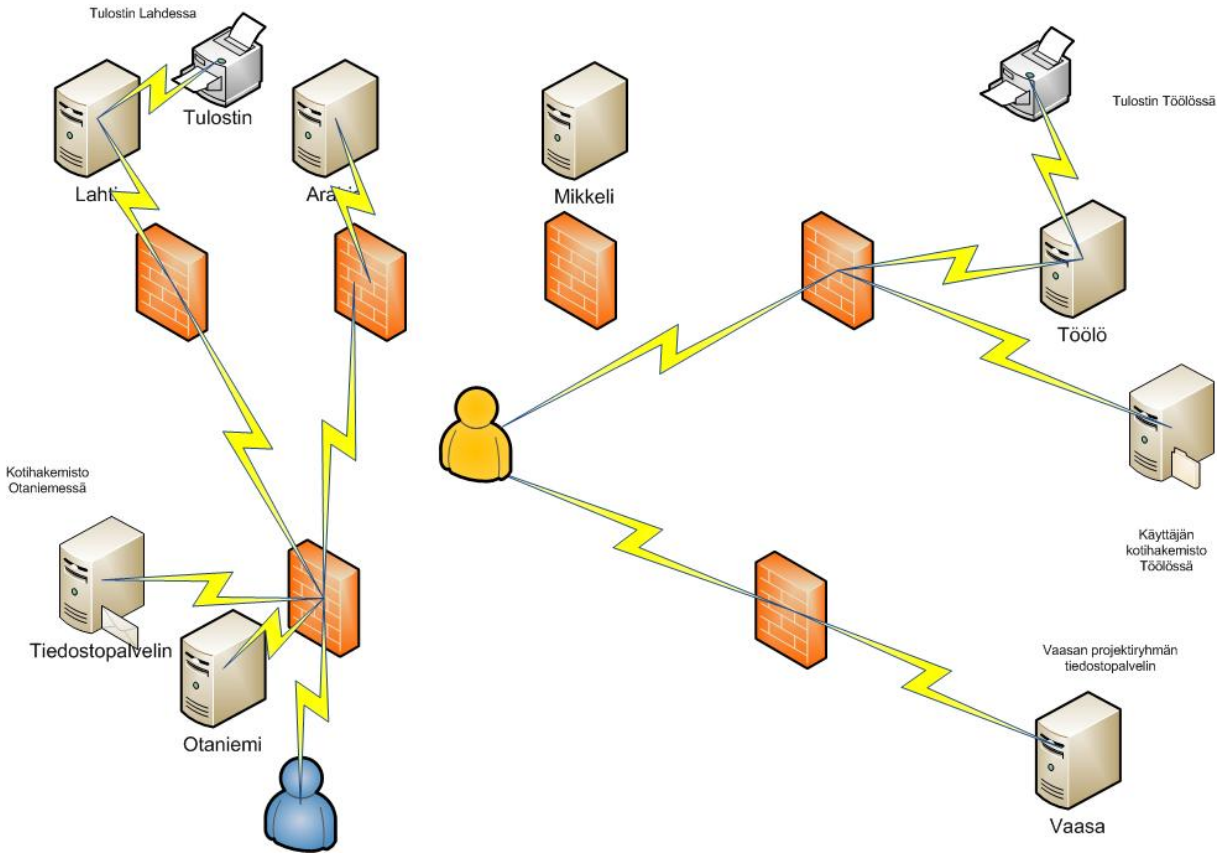
8.3 Hajauttamisen vaikutuksia

Hajauttamalla reititys kampuksille voidaan varmistaa välttämättömien palvelujen toiminta verkkoyhteyksien katketessa konesaleihin. Kysymys on enemmän periaatteellinen ja taloudel-

linen kuin tekninen. Palveluiden hajauttaminen lisää kustannuksia laitehankintoina ja ylläpitotyönä.

Liikkuvat käyttäjät käyttävät palveluita hajautetussa mallissa aina oman kampuksen palvelimilta. Vieraillessaan toisella kampuksella voi liikenne kulkea konesalien läpi kampukselta toiselle. Palveluiden ja reitityksen hajauttaminen kampuksille lisää haasteita palomuurisääntöjä suunnitellessa.

Palvelun sijoittaminen vain muutamaan konesaliin helpottaa palvelun suunnittelua, mutta edellyttää yhteyksien toimintaa kampuksien ja konesalien välillä. Konesaleille voidaan tehdä yhteisiä palveluverkkoja L2-tasolla. Tämän avulla palveluita voidaan halutessaan siirtää konesalista toiseen virtuaalisesti tai ihan palvelinlaitteilla levyjärjestelmän avulla muuttamatta palvelimen verkkoasetuksia. Tähän verkkoon voidaan tehdä tarvittavat palomuuriavaukset ja tilanne on vielä hallittavissa.



Kuva 4 Palomuuriavauksien esimerkki

Kuvassa 4 on kaksi eri käyttäjää ja heidän käyttötilanteessaan palomuuriavaukset alkavat jo olla vaikeammin määriteltäviä, kun aliverkkojen määrä kasvaa. Käyttäjien liikkuessa kampukselta toiselle on kaikkien verkkojen avauksien huomioiminen jo todella monimutkaista.

Reitityksen hajauttaminen palvelee hyvin kun käyttäjät pysyvät paikoillaan ja kampusten väliset yhteydet ovat epäluotettavia. Kunnon reititin on merkittävästi kalliimpi kuin kytkin. Funet pystyy tarjoamaan nopeita verkkoyhteyksiä valopolkuina kampuksille. Se parantaa toimintavarmuutta ja alentaa kustannuksia.

8.4 Sisäinen reititysprotokolla

Usean reitittimen verkossa on perusteltua käyttää sisäistä reititysprotokollaa eli IGP:tä (Interior Gateway Protocol). Esimerkkejä näistä protokollista ovat IS-IS [31] ja OSPF. IGP:n tehtävä on ylläpitää topologiaa reitittimien välisistä yhteyksistä automaattisesti. Tieto linkin katkeamisesta välittyy nopeasti eteenpäin ja liikenne voidaan ohjata toista reittiä.

IS-IS käyttää ISO-osoitteita eikä ole riippuvainen IP-osoitteista. Tämä on yleensä pelkästään hyvä asia. IS-IS on linkkitilaprotokolla ja se käyttää lyhyimmän polun viritykseen Dijkstran algoritmia. IS-IS tukee kahta eri tasoa. Level 1 tarkoittaa niitä reitittimiä, jotka reitittävät alueen sisällä. Level 2 tarkoittaa niitä jotka voivat reitittää alueiden välillä ja myös AS:n (autonomous system) ulkopuolelle. IS-IS pidetään hyvin skaalautuvana suuriin verkkoihin. Tämän vuoksi IS-IS on ollut suosittu suurien operaattoreiden verkoissa.

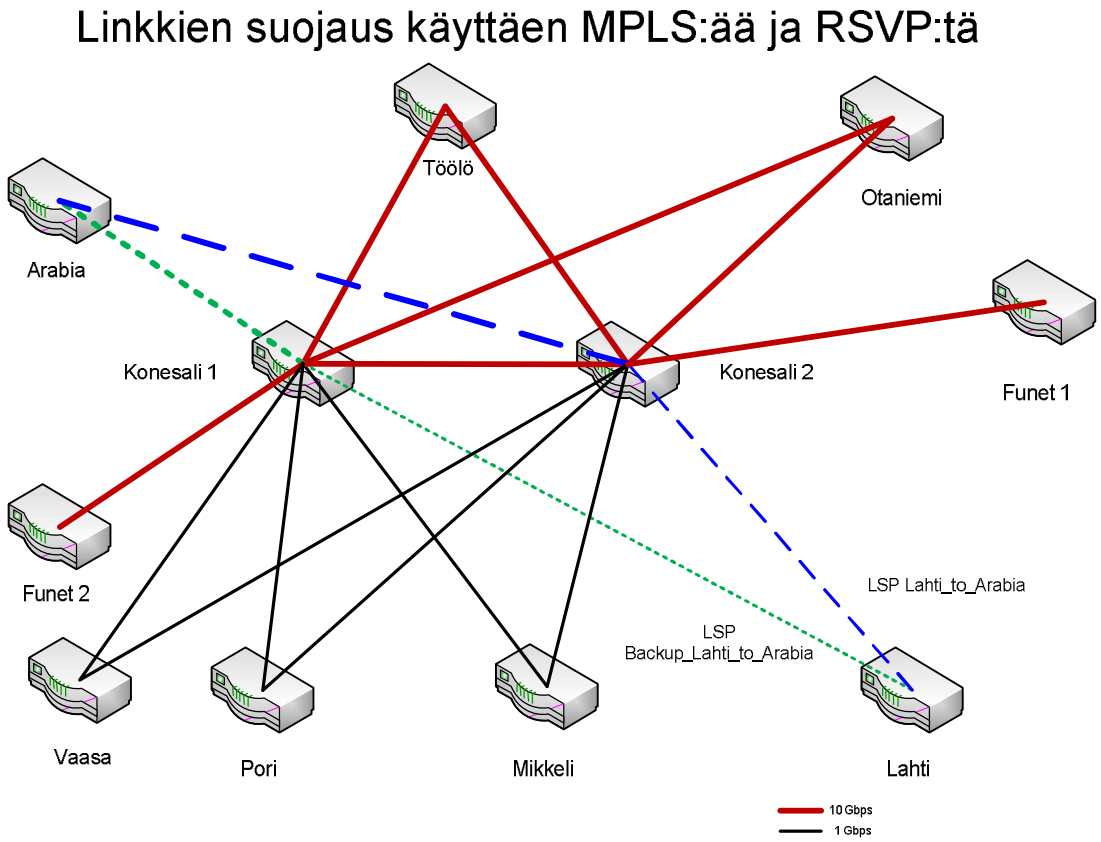
OSPF käyttää IP-osoitteita ja on hyvin yleinen yritysverkoissa. OSPF on pitkälle optimoitu ja siksi se on myös hyvin monimutkainen. OSPF on linkkitilaprotokolla ja myös se käyttää Dijkstran algoritmia lyhyimmän polun löytämiseen. OSPF etsii reitin IP-paketin kohdeosoitteen perusteella.

8.5 RSVP

RSVP (Resource reservation protocol) [32] huolehtii verkkoresurssien käyttöönotosta ja hallinnasta. Sen avulla MPLS signaloidaan avaamaan LSP (label switched path) haluttujen reitittimien väliin. RSVP:llä voi varata tietyn kaistanleveyden tai muuttaa muita palvelunlaadun ominaisuuksia. RSVP-TE (Traffic Engineering) antaa lisää mahdollisuuksia LSP:n määritte-

lyyn. Polku voidaan pakottaa kulkemaan jotain tiettyä reittiä, jota IGP ei normaalisti valitsisi. Näitä käsin asetettuja polkuja tavallisesti vältetään, koska ne teettävät ylimääräistä työtä suunnittelussa ja ylläpidossa. Samalla IGP:n tuoma automaattinen reittien päivitys kärsii käsin asetetuista poluista.

8.6 Linkkien suojaus



Kuva 5 Linkkien suojaus

Kuvassa 5 on tehty LSP Lahdesta Arabiaan käyttäen linkkisuojausta. Ensisijaisesti liikenne kulkee konesali 2:n kautta ja sitä kuvaa sininen katkoviiva. Varayhteys on merkitty vihreällä katkoviivalla. IGP ylläpitää tietoa verkon rakenteesta. Heti kun se tai RSVP huomaa yhteyden katkenneen liikenne alkaa kulkea varareittiä pitkin konesali 1:n läpi. Liikenteen uudelleenohjaukseen kuluu IGP:n sisäisin keinoin muutamia sekunteja.

Linkkisuojaus määritellään jo alkuvaiheessa niille yhteyksille, jotka halutaan varmistaa ja joiden kohdalla ei haluta odottaa LSP:n uudelleen signalointia. Suurissa operaattoriverkoissa

linkkisuojausta käytetään erityisesti, jos asiakkaalle myyty palvelutaso ei salli katkoja. Aalto-yliopiston verkko ei kasva niin suureksi, ettei linkkisuojausta voitaisi käyttää.

8.7 BFD

Nopea linkin vikaantumisen havaitseminen on tärkeää kaikille verkon osille. Ethernet ei luonnostaan tue etäpään vian tunnistamista, vaan sitä varten tarvitaan erillisiä mekanismeja. Yleisin tapa on luottaa sisäreititysprotokollan (IGP) hello-viesteihin linkkivikojen tunnistamisessa. Niiden avulla vian huomaamiseen saattaa kulua sekunteja. IGP-protokollien vianhallinta on suhteellisen raskas toimenpide ja siksi vianhavainnointiin on kehitetty yleisesti ja eri tarkoituksiin sopiva tekniikka.

BFD:tä (Birectional Forwarding detection) [33] käytetään nopeuttamaan linkkivikojen huomaamista. Sen toiminta perustuu kahdensuuntaiseen valvontaan. BFD asiakas eli reititin jossa on BFD asetettu linkille, aloittaa lähettämällä määräajoin kontrolliviestejä toiselle osapuolelle (peer). Kontrolliviestien sisältönä kerrotaan BFD:n parametrit. Niitä ovat lähetysaikaväli (Transmit Interval) ja vastaanottoaikaväli (Receive Interval). Lisäksi ilmoitetaan tunnistamisen kerroin (Detection Multiplier). Yhdessä näiden perustietojen perusteella voidaan arvioida linkkivian havaitsemiseen ja uuden reitin valintaan kuluvaa aikaa.

Lähetysaikaväli päätellään lopullisesti vertailemalla osapuolten lähetysaikavälejä vastaanottoaikaväleihin. Luvuista suurempi valitaan lähetysaikaväliksi kyseiselle linkille.

Reititin	Lähetysaikaväli (ms)	Vastaanottoaikaväli (ms)
A	200	250
B	225	225

Neuvottelun tuloksena A vertaa omaa 200 ms lähetysaikaväliä B:n 225 ms vastaanottoaikaväliin ja neuvotelluksi lähetysaikaväliksi valitaan suurempi 225 ms. B:n lähetysaikaväli 225 ms on pienempi kuin A:n vastaanottoaikaväli 250 ms. 250 ms valitaan neuvotelluksi lähetysaikaväliksi B:lle. Tunnistamisen kerroin asetetaan haluttuun arvoon.

Reititin	Neuvoteltu lähetysaikaväli (ms)	Tunnistamisen kerroin	Kunnon tunnistamisen aikaväli (ms)
A	225	2	750
B	250	3	450

Lopputuloksena reititin A huomaa linkin B:hen olevan poikki 450 ms ja B huomaa yhteyden A:han olevan poikki 750 ms kuluttua.

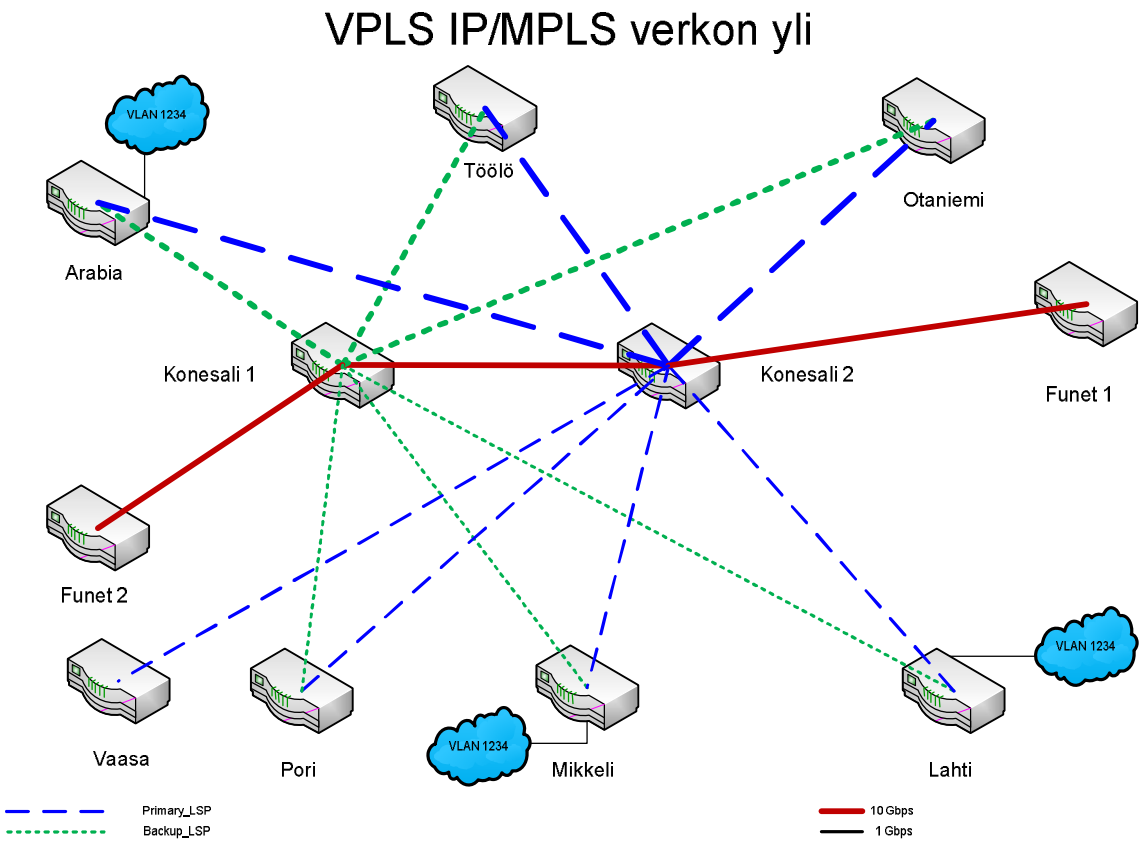
8.8 BGP

BGP (Border Gateway Protocol) [34] on tarkoitettu oman verkkoalueen eli AS:n (Autonomous System) ja ulkopuolisten AS:ien välisten reittien hallintaan. Suurissa verkoissa sisäisesti käytetään iBGP:tä (Interior Border Gateway Protocol). Kaikilla iBGP reitittimillä AS:n sisällä on BGP sessio toistensa kanssa (full mesh). Tämä voi olla skaalautuvuusongelma erityisesti suurissa verkoissa. Niissä voidaan käyttää BGP:n Route reflectoreita (RR) tai Confederointia hallinnoinnin helpottamiseksi. RR on yksi tai useampi reitittimistä, joka ottaa vastaan kaikkien samaan klusteriin kuuluvien reitittimien reittitiedot. Lopputuloksena iBGP reitittimet liikennöivät RR:n kanssa ja saavat sieltä reititystiedot.

Confederointi mahdollistaa suuren operaattoriverkon AS:n pilkkomisen pienempiin AS:iin. Tämä tilanne voi tulla luonnostaan eteen kun operaattorien tai yritysten liiketoiminnat yhdistyvät. Confederoinnin hyötynä ovat pienempi iBGP mesh eli pienempi joukko reitittimiä välittää BGP-liikennettä toisilleen, mutta ulospäin kaikki näkyvät yhtenä AS:nä.

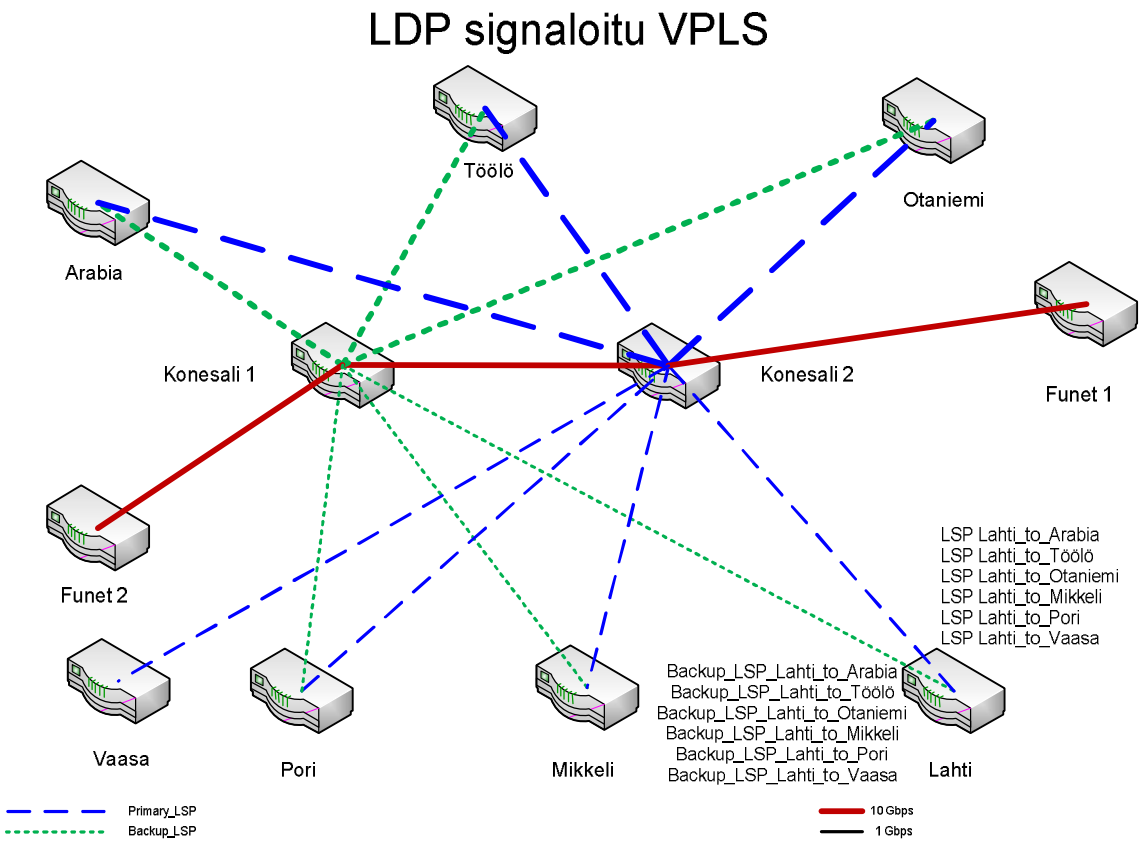
8.9 VPLS

VPLS (Virtual Private LAN Service) [35] on operaattoreiden käyttämä tekniikka, jossa hyödynnetään olemassa olevaa IP/MPLS verkkoa asiakkaiden L2VPN:nien toteuttamiseen. VPLS:n ohjaamiseksi on kaksi eri standardia. RFC 4671 määrittelee BGP signaloidun VPLS:n. Sen vahvuutena on Autodiscovery. RFC 4672 määrittelee LDP (Label Distribution Protocol) signaloidun VPLS:n. Se edellyttää käsin määrittelyä jokaisen PE (Provider Edge) reitittimen jälkeen. PE reitittimen takana on asiakkaan verkkoja.



Kuva 6 VPLS IP/MPLS verkon yli

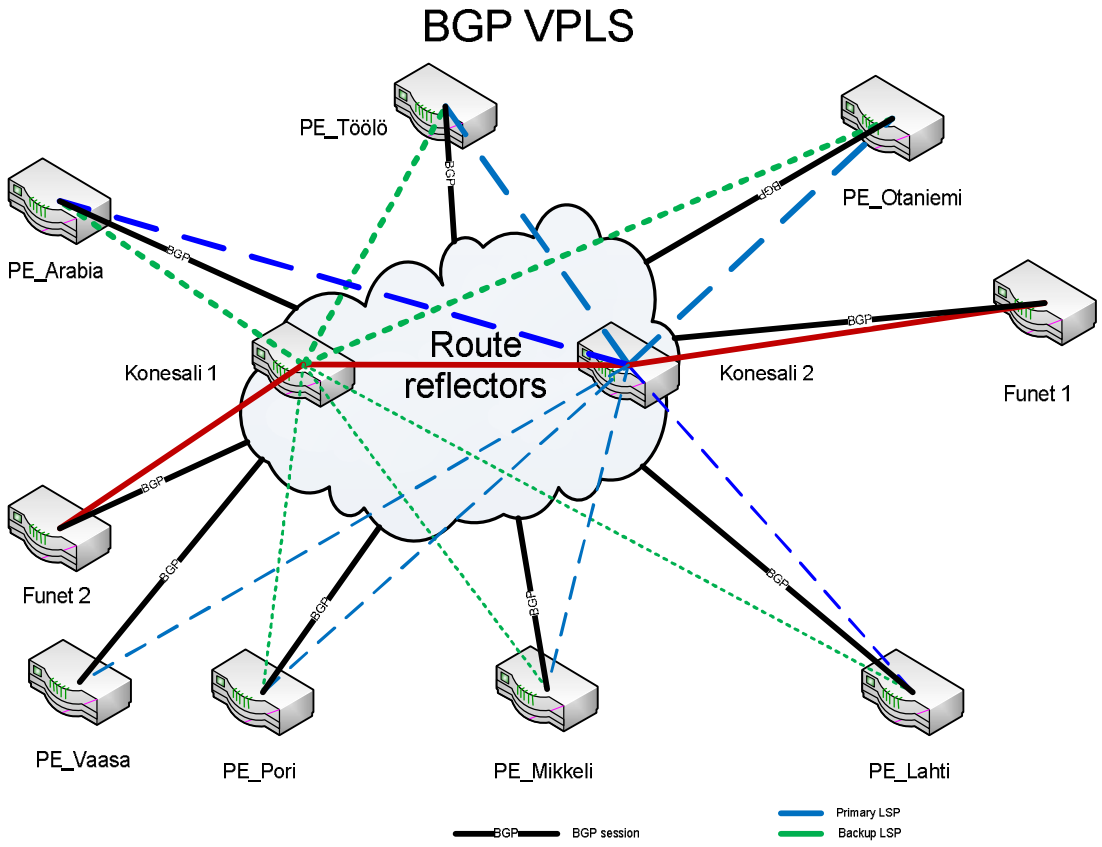
VPLS:n keinoin voidaan sama aliverkko näyttää eri PE-reitittimien takana. Reititetyssä verkossa tämä ei ole mahdollista päästämällä VLAN:eja läpi linkeille. VPLS toimii käyttäjän näkökulmasta kuin normaali ethernet. MAC-osoite (Media Access Control) näkyy PE-reitittimen MAC-osoitetaulussa ja osoittaa tietyn PE-reitittimen suuntaan. Tuntemattoman osoitteen tapauksessa kysely lähetetään kaikkien PE-reitittimien suuntaan. Kun vastaus saadaan, tieto päivitetään PE-reitittimien MAC-osoitetauluun.



Kuva 7 VPLS LSP:t manuaalisesti syötettynä

Kuvassa 7 on esimerkkinä lueteltu kaikki LSP:t joita tarvitaan VPLS:n määrittelemiseksi LDP:n keinoin pelkästään Lahdesta käsin. Sama toistuu uudestaan kaikilla kampuksilla. LDP sessio tarvitaan jokaisen PE-reitittimen väliin. Uuden PE-reitittimen lisääminen edellyttää kaikkien PE-reitittimien päivittämistä. Tieto pitäisi ylläpitää käsin erillisessä taulukossa tai jollain muulla tavalla. LDP signalointi soveltuu pieniin ympäristöihin.

Automatisointia varten BGP VPLS:ssä on Autodiscovery-toiminto. Se käyttää BGP Route Reflectoreita (RR) VPLS:n tarvitsemien tietojen välittämiseen. Autodiscoveryn ominaisuudet korostuvat suurissa ympäristöissä. PE-reitittimen lisääminen verkkoon edellyttää ainoastaan BGP-sessiota RR:n. Sieltä tieto PE:stä ja sen takana olevista verkoista leviää eteenpäin muille PE-reitittimille. BGP:n signaloimana VPLS:n tarvitsemat LSP:t muodostetaan automaattisesti eikä niitä tarvitse ylläpitää erikseen lainkaan. Käytettäessä MPLS:ää BGP on merkittävässä roolissa.

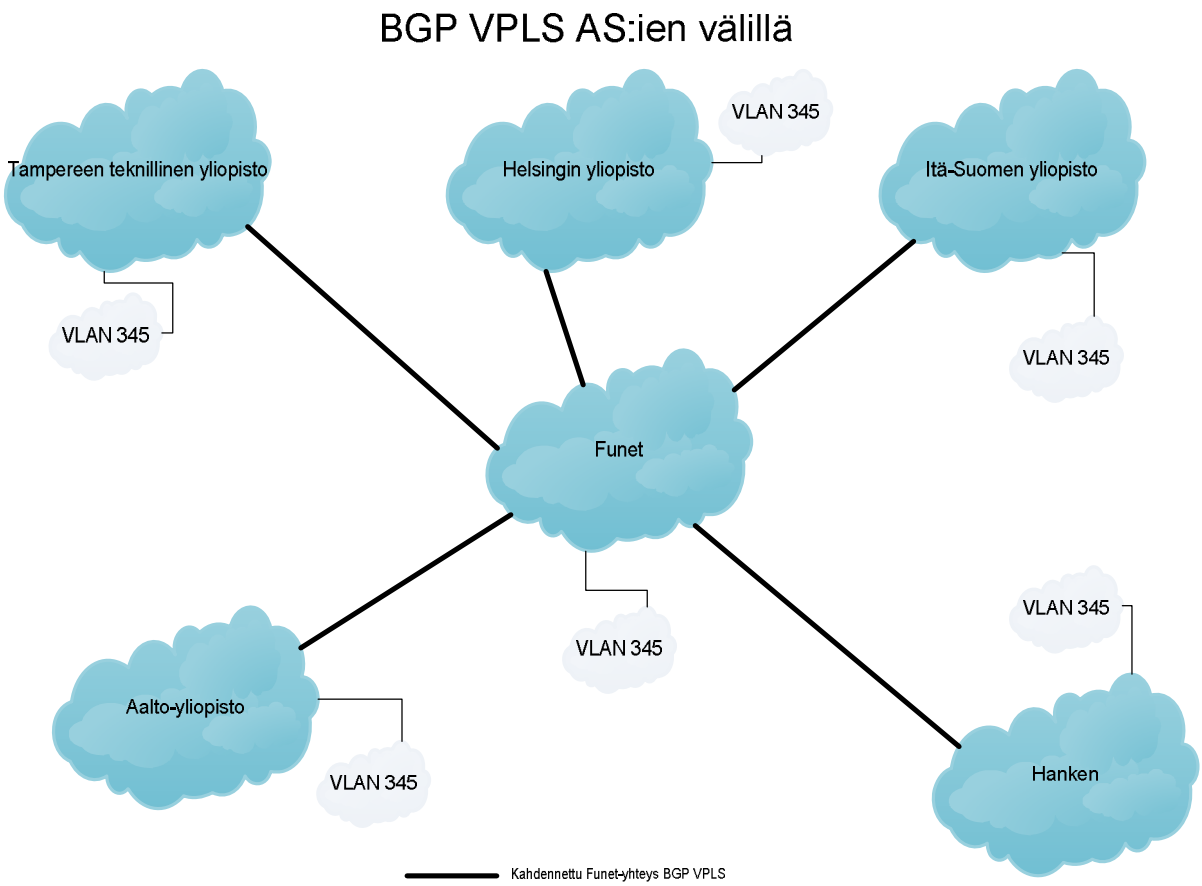


Kuva 8 BGP VPLS

BGP VPLS:n keinoin PE-reitittimen lisääminen edellyttää BGP-sessiota ainoastaan Route reflectoreihin. Niiden kautta kaikki muut laitteet saavat tiedon uudesta PE:stä ja tarvittavat LSP:t muodostetaan automaattisesti.

BGP VPLS antaa mahdollisuuden tehdä organisaatioiden välisiä L2VPN:iä esimerkiksi tutkimusryhmille, jotka toimivat eri yliopistoissa. Käyttämällä Route Targetia voidaan tieto VPLS instanssista välittää tiedon AS:stä BGP:n Route target extended community attribuutissa. Niitä attribuutteja käytetään tunnistamaan VPN:n sijainnit (site) ja välittämään VRF-instanssit (Virtual Routing and Forwarding).

Käytännössä VPLS laajentaa BGP:n avulla mahdollisuuksia perinteisen reitityksen ulkopuolelle. BGP VPLS olisi erinomainen työkalu yliopistoverkkoja ylläpitävälle Funetille. Yhteistyö muiden yliopistoverkko-operaattoreiden kanssa voisi tuoda BGP VPLS:lle yllättäviä käyttötarkoituksia.



Kuva 9 BGP VPLS yliopistojen välillä

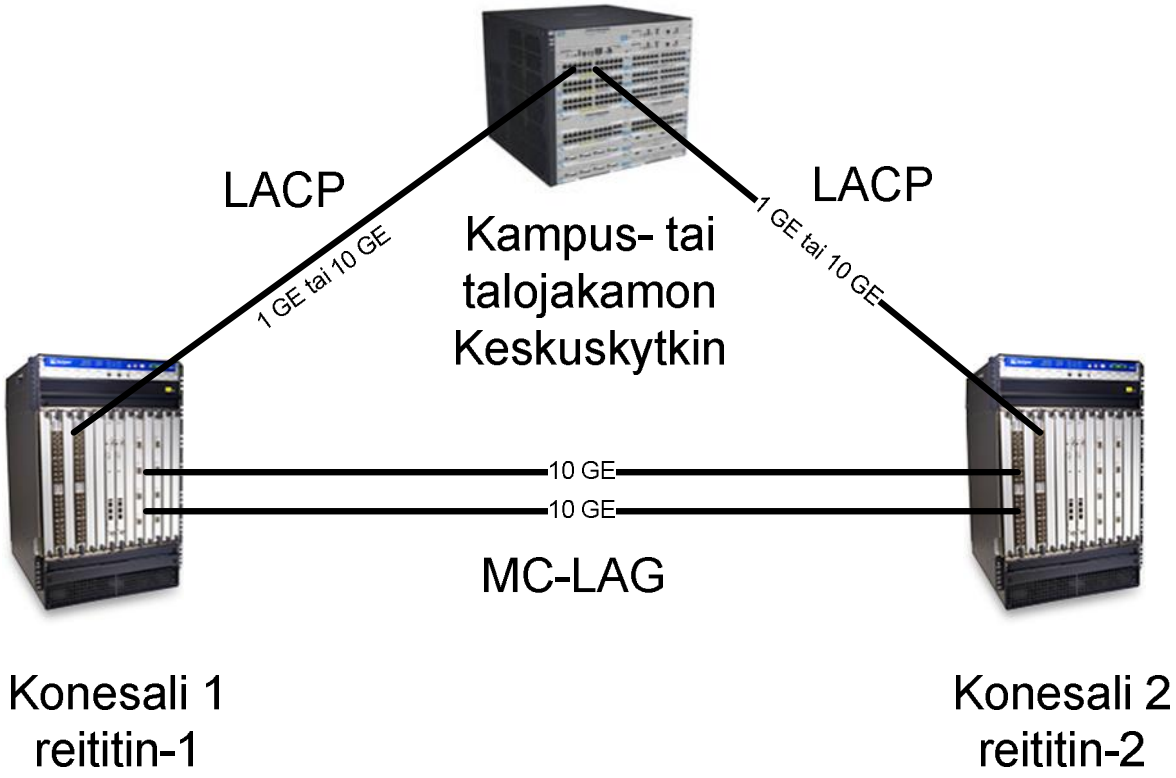
Kuvassa 9 BGP VPLS:n avulla on tehty organisaatioiden välinen tutkimusverkko VLAN 345. Siinä organisaatiorajoista ja AS:stä huolimatta on tehty yhteinen L2-verkko viiden yliopiston ja Funetin kesken. Käyttötarkoituksia tällaiselle voi keksiä useita, mutta esimerkkeinä yhteinen palveluverkko, työasemien verkkovierailu, suljettu L2-tutkimusverkko ja yhteinen mittalaiteverkko.

VPLS:n käyttö tuo paljon uusia mahdollisuuksia ja ulottuvuuksia perinteiseen IP-verkkoon. Multicast on haaste kaikille verkoille. MPLS:n luomat LSP:t tukkeutuisivat Multicast-liikenteestä, ellei tähän tarkoitukseen olisi kehitetty P2MP (Point to MultiPoint) LSP:eitä. Niiden avulla liikenteen kopiointi tapahtuu mahdollisimman kevyesti. Tämä ominaisuus on kehitetty operaattoreiden toiveesta erityisesti IPTV:n (Internet Protocol Television) tarpeisiin.

9 Arkkitehtuurivaihtoehto 2 - Keskitetty reititys

9.1 Reititys keskitettynä kahteen konesaliin

Tässä luvussa käsitellään yksinkertaistettua versiota verkon rakenteesta. Kaikki palvelut ja reititys on keskitetty kahteen konesaliin. Keskittämisellä on vaikutuksia verkon toimintaan monella tasolla. Muuttamalla verkon rakenne yksinkertaiseksi ja hajauttamalla yhteydet järkevästi voi kohtuullisilla kustannuksilla saada nopean ja helposti laajennettavan verkon.

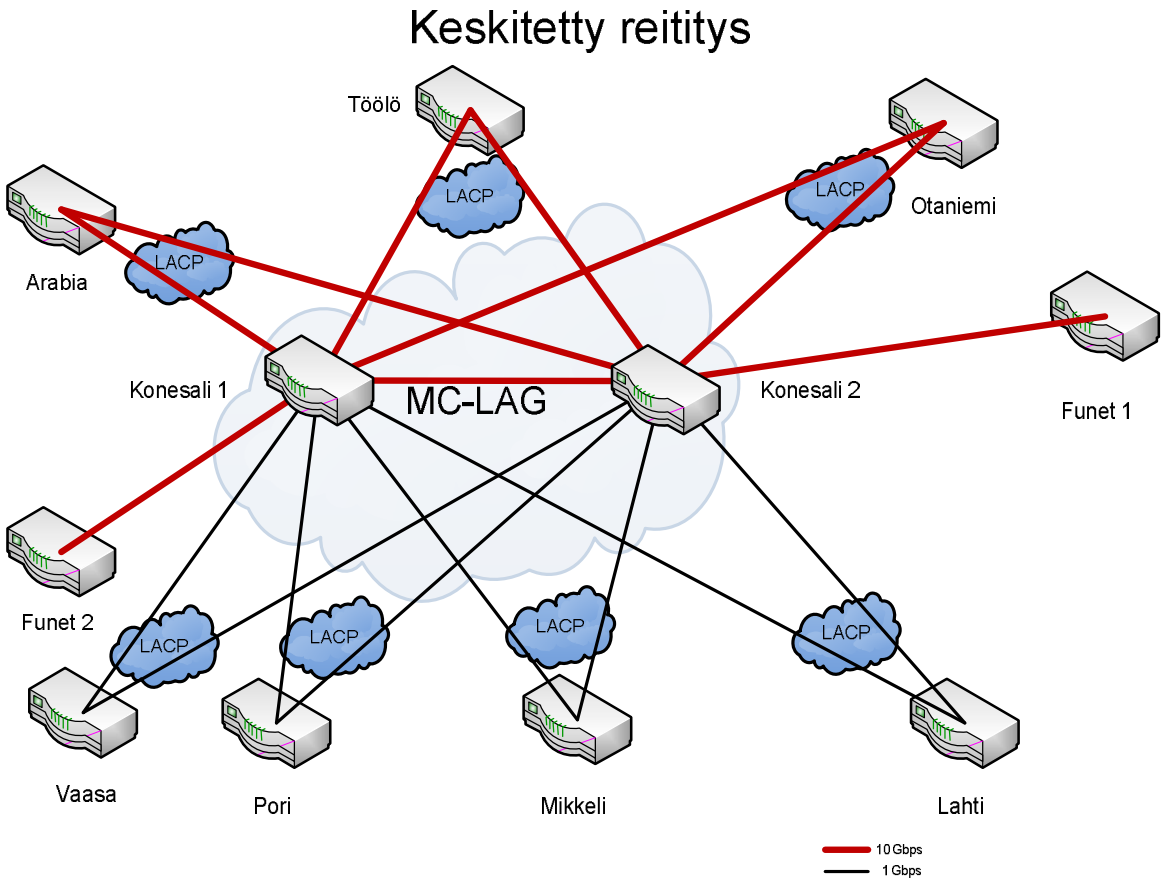


Kuva 10 Keskuskytkinten yhteydet konesaleihin

Mallissa jokaiselle kampukselle tai suurilla kampuksilla eri rakennuksiin voidaan rakentaa kahdennettu runkoverkko. Käyttämällä kahta eri valokaapeliyhteyttä tuodaan yksi yhteys molempiin konesaleihin. Molemmissa konesaleissa on yksi reititin, johon yhteys kytketään.

Kuvassa 10 on havainnollistettu yhden kampusrunkokytkimen avulla miten verkko rakentuu. Kampuksilla on ainoastaan kytkimiä. Reitittimiä on vain kaksi koko yliopiston verkkoa var-

ten, yksi molemmissa konesaleissa. Reitittimet varmentavat toisiaan ja kaikki liikenne kulkee niiden kautta.



Kuva 11 Keskitetty reititys, MC-LAG ja LACP

Reitittimien välille on muodostettu MC-LAG (Multi-chassis link aggregation group). Sen avulla voidaan yhdistää kahteen eri reitittimeen LACP-yhteyksiä (Link aggregation control protocol). Keskuskytkimiä sijoitetaan keskeisiin tietoliikenteen solmukohtiin. Tällaisia ovat kampuksien pääjakamot ja suurimpien talojen jakamot. LACP:tä käyttämällä voidaan hyödyntää molempia linkkejä kuormantasaukseen. Toisen linkin vikaantuessa liikenne kulkee automaattisesti vain ehjää linkkiä pitkin.

Verkon rakenne on yksinkertainen ja vianselvitys helppoa. Tilanteessa, jossa etäkampuksen yhteys ei toimi, voidaan sulkea linkki kerrallaan yhteys etäkampukselle. Vianselvitys etenee sulkemalla pois mahdollisia vian aiheuttajia.

Kytkinverkon hallinnointi on yksinkertaista ja siihen on kehitetty paljon erilaisia mekanismeja. Yksi työllistävä ja virheitä aiheuttava kohta on VLANien määrittely kytkimiin. Ne voidaan määritellä automaattisesti käyttäen GVRP-protokollaa. Se ylläpitää kytkimissä automaattisesti listaa VLANeista. Kytkinmallikohtaiset rajoitukset VLANien määristä ja GVRP:n ominaisuuksista pitää huomioida laitteita hankittaessa.

9.2 LACP:n vaatimukset

LACP (Link Aggregation Control Protocol) on vuonna 2000 esitelty vakiintunut tekniikka. Sitä on kehitetty vuosien ajan ja yhteensopivuus eri laitevalmistajien kesken on hyvä. LACP on pidetty yksinkertaisena. LACP yhdistää saman nopeuksisia linkkejä yhteen ja muodostaa niistä yhden kuormantasausta tukevan kanavan. LACP on pitkään toiminut vain kahden laitteen välillä, mutta nykyaikaisissa reitittimissä on tuki MC-LAGille. Sen myötä STP:n (Spanning Tree Protocol) voi korvata kokonaan LACP:llä.

STP oli aikaisemmin ainoa vaihtoehto L2 -varayhteyksien tekemiseen. Sen suurin heikkous on kuormantasauksen puute. Toinen yhteys on koko ajan käyttämättömänä eikä sitä voi mitenkään hyödyntää saman VLANin kuljettamiseen.

LACP edellyttää, että linkkien on oltava yhtä nopeita ja kaksisuuntaisia (full duplex). Järkevät vaihtoehdot ovat siis 1 GE (Gigabit Ethernet) ja 10 GE. Käytössä on jo valmiiksi kahdennetut valopolut etäkampuksille. Niiden yhdistäminen LACP:n avulla on edullinen ja tehokas keino. LACP on tuettuna useimmissa kytkimissä ja kaikissa keskuskytkimeksi sopivissa laitteissa.

LACP ei ota kantaa vaikka yhteydet olisi toteutettu eri tekniikoilla. Toinen yhteys voi olla CWDM (Coarse Wavelength-Division Multiplexing) valopolku, joka kiertää pitkän matkan ja toinen yhteys voi olla kategoria 6 parikaapeli. Yhteyksiä voi olla enemmän kuin kaksi laitevalmistajasta riippuen.

9.3 Kaksi reititintä varmentamassa toisiaan

Keskittämällä kaikki yhteydet kahteen reitittimeen voidaan tehdä samantasoiset yhteydet etäkampuksille vaikka maantieteellinen etäisyys on suuri. Jokaiseen aliverkkoon voidaan esimerkiksi VRRP:llä (virtual router redundancy protocol) [36] toteuttaa kahdennus reititykselle.

Reitittimet huolehtivat automaattisesti kumpi niistä on aktiivinen. VRRP:n kaltaisia tekniikoita on reititinvalmistajilla muitakin, mutta VRRP on yleisesti tunnettu standardi.

Kahdennettu reititin näkyy verkossa oleville tietokoneille yhtenä virtuaalisena oletusyhdyskäytävänä. Molemmilla reitittimillä on oma kiinteä osoitteensa, mutta lisäksi on yhteinen virtuaalinen reitittimen osoite. Osoite siirtyy toiselle reitittimelle jos ensisijainen reititin vikaantuu.

Kahteen konesaliin keskitetty malli kannustaa sijoittamaan myös palvelimet vain kahteen konesaliin. Hajauttaminen kahteen on tyypillisesti paljon helpompi toteuttaa kuin hajauttaminen kolmeen tai useampaan konesaliin. Konesalien väliin tarvitaan riittävät yhteydet reitittimien välisen liikenteen ja esimerkiksi levyliikenteen hoitamiseksi.

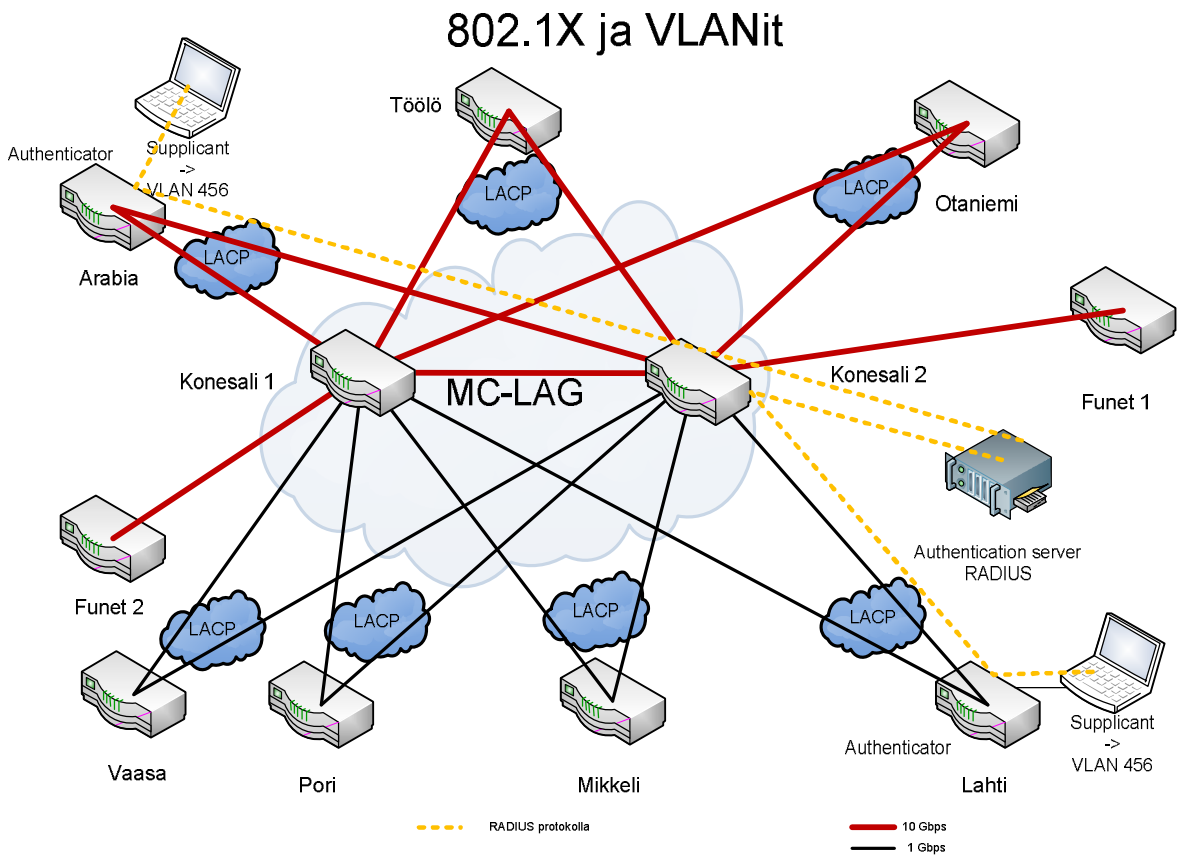
9.4 Kahdennettu Internet-yhteys

Molemmista konesaleista pitäisi lähteä 10 GE -yhteys ulos Funetiin. Häiriötilanteessa riittäisi kun toinen niistä on toimintakunnossa. Ulospäin käytetään BGP -reititysprotokollaa. Se huolehtii automaattisesti kumpi 10 GE – linkeistä on käytössä. Funetin periaatteen mukaan yliopistoille näytetään vain oletusreitti Internetin suuntaan.

Aalto-yliopiston verkon topologiaa ylläpidetään IS-IS protokollalla. Sen avulla reitittimillä on tieto toistensa tilasta. BFD:llä (Bidirectional Forwarding Detection) reitittimien välisten yhteyksien seurantaa voidaan nopeuttaa ja ajastimia säätää halutun mukaiseksi. Tämä tieto välittyy nopeasti BGP:lle joka taas vaikuttaa ulospäin menevän liikenteen ohjautumiseen.

9.5 Keskitetyn reitityksen etuja

Keskitetyssä mallissa VLAN:ien (Virtual LAN) käyttö kampuksien välillä onnistuu helposti. VLAN:n määrä on 802.1Q standardin määrittelemänä korkeintaan 4096. Useat halvemmat kytkinmallit tukevat vain rajattua määrää yhtäaikaisia VLAN:a. Saman VLAN:n käyttö eri kampuksilla helpottaa merkittävästi esimerkiksi porttiautentikoinnin 802.1X käyttöä. Kone voi saada samat IP-asetukset kampuksesta riippumatta. Tämä edellyttää 802.1X:ää tukevien VLANien määrittelyä kaikkiin mahdollisiin kytkimiin joissa se on käytössä.



Kuva 12 802.1X porttiautentikointi

Kuvassa 12 näytetään miten kannettava tietokone tunnistautuu verkkoon konevarmenteella. Tunnistautumisen jälkeen RADIUS-palvelin lähettää kytkimelle koneelle kuuluvan VLAN ID:n. Olennaista on, että saman VLANin voi saada millä tahansa kampuksella. Rasiat voisi merkitä kuvaavasti kirjaimella ”X”. 802.1X vaatii toimiakseen PKI-järjestelmän. Työasemalle on haettu konekohtainen varmenne, jolla se tunnistautuu kytkimelle. Lisäksi käyttäjältä kysytään käyttäjätunnus ja salasana.

Keskitetyssä reitityksessä kaikki liikenne kulkee konesalien kautta. Käyttäjän varayhteyksien rakentaminen on helpompaa kuin Internetin kautta pääsee aina VPN:llä suoraan verkon palveluihin. VPN toimii myös siinä kun kampusverkkoyhteys on jostain syystä katkennut. Palveluiden toiminta ei enää ole riippuvainen sekä kampuksen, että konesalien palveluista. Keskittäminen helpottaa ylläpitämistä ja vähentää kustannuksia. Osaavaa ylläpitohenkilökuntaa voidaan hyödyntää tehokkaasti kun järjestelmä on riittävän suuri ja keskitetty. Kampuksien konesalien ylläpitäminen on kallista ja aikaa kuluu siirtymiseen paikasta toiseen.

Nykypäivän hallintatekniikat sallivat konesalin sijoittamisen pitkien välimatkojen päähän. Suurin ratkaistava asia on varayhteyksien rakentaminen. Palvelimet voidaan ostaa täyteen kalustetuissa palvelinkehikoissa ja niitä otetaan käyttöön tarpeen mukaan. Virtualisoimalla saadaan vähän suorituskykyä tarvitsevat palvelut pois erillisistä palvelinlaitteista.

Keskitetyn reitityksen tuomat kustannussäästöt ovat merkittäviä. Karkea nyrkkisääntö on, että reitittimen portti maksaa kymmenen kertaa enemmän kuin kytkimen portti. Esimerkkinä Juniperin MX960 10 GE portti maksaa noin 6000 EUR ja HP:n procurve 8212zl:n 10 GE portti maksaa noin 600 EUR.

9.6 Laitevaatimukset

Konesalien reitittimien valinta vaatii huolellista selvitystyötä. Suurimmilta valmistajilta löytyy reitittimiä, joissa MC-LAG on tuettuna. Kokonaisuudessaan ominaisuuksia tarvitaan niin paljon, että huolellinen testaus on välttämätöntä ennen hankintapäätöksen tekoa. Valmistajan lupauksiin ei voi sokeasti luottaa eikä riitä, että asia mainitaan tarjouskilpailussa.

Onnistuneella ominaisuuksien määrittelyllä kustannustehokas verkko voi olla hankintahinnaltaan hieman kalliimpi, mutta ylläpidettävyydeltään ja elinkaareltaan merkittävästi parempi. Laitevalmistajan myöntämä takuu ja huoltovarmuus ovat kriittisiä asioita. Lyhyen elinkaaren laitteita ei kannata edes tutkia tarkkaan. Niiden tuotekehityksen ja ohjelmistopäivitysten loppumisesta voi jo etukäteen olla varma.

Useat laitevalmistajat ovat siirtyneet käyttämään optisten komponenttien tunnistusta eli kytkin tai reititin ei suostu toimimaan muiden toimittajien optiikoiden kanssa. Sama suuntaus on sekä 1 GE SFP (Small Form-Factor Pluggable), että 10 GE SFP+ (SFP Small Form-Factor Pluggable +) optiikoissa.

SFP ja SFP+ ovat identtisiä ulkoiselta rakenteeltaan ja joissain laitteissa molemmat vaihtoehdot toimivat samassa liittimessä. Ylläpitäjä voi optiikan valinnalla vaikuttaa toimiiko verkko 1 GE vai 10 GE nopeudella. Optiikoiden hinnoissa on vielä suuria eroja, mutta vähitellen hinnat laskevat 10 GE osalta niin lähelle 1 GE hintoja, että sillä ei kustannusmielessä ole enää merkitystä erityisesti runkoverkon yhteyksissä.

9.7 Ethernet OAM

Kehittyneimmät laitteet tukevat Ethernet OAM:ää (Operations, Administration, and Management). [37] Sen tavoitteena on tuoda Ethernetiin siitä puuttuvia hallinta ja valvontaominaisuuksia. OAM:n ominaisuuksia:

- Automaattinen verkonvalvonta
- Auttaa vianselvityksessä ja paikantamisessa
- Helpottaa ymmärtämään mihin palveluihin vika vaikuttaa
- Liikenteen määrän mittaaminen

OAM:stä on kaksi standardia IEEE 802.1ag ja ITU-T Y.1731. Molemmat toteuttavat nämä kolme ominaisuutta:

1. Vian huomaaminen (Fault Detection) CCM (Continuity Check Messages)
2. Vian varmistaminen (Fault verification) LBM (Loopback Messages)
3. Vian rajaaminen (Fault Isolation) LTM (Link Trace Messages)

ITU-T Y.1731 lisäksi vielä seuraavat ominaisuudet

1. Viasta tiedottaminen (Fault Notification) AIS (Alarm Indication Signal)
2. Kehyksen katoamissuhde (Frame Loss Ratio)
3. Kehyksen viive (Frame Delay)
4. Kehyksen viiveen vaihtelu (Frame Delay Variation)

10 Arkkitehtuurimallien vertailu ja analyysi

10.1 Ominaisuuksien vertailu

Keskitetyn ja hajautetun reitityksen välillä on paljon erilaisia vivahde-eroja. Siksi tässä diplomityössä on kärjistäen verrattu ääripäitä. Molemmilla ratkaisuilla verkko saadaan toimimaan, mutta vaikutuksien tasapuolinen arviointi ei ole mahdollista ilman vuosien rinnakkaista testaamista. Arvioinnissa joudutaan tyytymään hyvien ja huonojen puolien luettelemiseen ja asiantuntijahaastattelujen perusteella tehtävään arvioon.

Huomioitava asia	**Hajautettu arkkitehtuuri**	**Keskitetty arkkitehtuuri**
Kustannukset	noin 5 kertaa kalliimpi kampuksilla	Edullinen
Kahdennus	1. Sisäreititysprotokolla (OSPF tai IS-IS) huolehtii uuden reitin. 2. MPLS linkkisuojaus	1. Linkkien yhdistäminen kampuskytkimestä kahteen reitittimeen käyttäen LACP ja MC-LAG protokollia. 2. Spanning tree protokolla. Heikkoutena kuormantasaus.
Kuormantasaus	Toimii ECMP:llä (Equal-cost Multipath) jos vaihtoehtoisten reittien kustannus on sama.	LACP tukee luonnostaan kuormantasausta.
Multicast	IP multicast -reititys ja MPLS verkoissa voidaan käyttää point to multipoint (P2MP) polkuja.	Multicast -liikenne voi olla kampuslinkeillä useaan kertaan rinnakkaisissa VLAN:eissa.
Verkon suunnittelu, toteutus ja ylläpito	Vaatii erityistä ammattitaitoa	Matalampi kynnys toteuttamiseen ja ylläpitoon
Palveluiden sijoittelu	Voidaan vapaasti sijoittaa kampuksille. Konesalien kustannukset pitää huomioida.	Kannattaa keskittää konesaleihin verkkoliikenteen ja kustannusten järkeistämisen takia.
Hallinnan helppous	Kestää kuukausia omaksua	Omaksuu viikoissa
Vikojen rajaaminen	Paljon ominaisuuksia ja vaikeat viat	Yksinkertainen ja L2 – kerroksen suojausmekanismit rajallisia

Taulukko 3 Arkkitehtuurimallien ominaisuuksien vertailu

Kustannuksien erot muodostuvat kampuksille tulevien laitteiden hinnoista. Konesalien reitittimet ovat samanlaisia molemmissa arkkitehtuurimalleissa eli niiden vaikutusta loppuhinnassa ei huomioida.

Kahdennus on helppo ja yksinkertainen keskitetyssä mallissa. Matalan tason protokolla LACP huolehtii linkkien yhdistämisestä ja vikatilanteessa liikenteen ohjauksesta toiselle linkille. Hajautetussa mallissa hyödynnetään IGP-protokollien keinoja kahdennukseen.

Kuormantasaus keskitetyssä mallissa hoidetaan MC-LAG:lla ja LACP:llä. Niiden toiminta on automaattisesti kuormaa tasaavaa. Hajautetussa mallissa kuormantasauksesta huolehditaan IGP:n avulla.

Multicast toimii molemmissa arkkitehtuurimalleissa moitteetta. Keskitetyssä mallissa on huomioitava se, että sama lähetys voi olla usealla linkillä samaan aikaan jos tilaajia on useassa aliverkossa. Hajautetussa mallissa tätä ongelmaa ei ole.

Verkon suunnittelu, toteutus ja ylläpito vaativat aina ammattitaitoa. Keskitetty malli on suoraviivainen ja helppo omaksua. Reitittimien ja kytkinten asetukset ovat hyvin samanlaisia kaikkialla. VLAN:ien levittäminen toimii helposti GVRP:llä. Hajautetussa mallissa ylläpidon pitää omaksua automatiikan hienoudet ja oppia vianselvitystä kehittyneiden protokollien kanssa. Kokonaisuus muodostuu seuraavista protokollista: IS-IS(IGP), RSVP, MPLS, BGP ja VPLS.

Palveluiden sijoittelu on tärkein osa verkon kokonaisuuden suunnittelua. Keskitetyssä mallissa tämä on hyvin suoraviivaista ja selkeää. Kaikki palvelut kahdennetaan ja sijoitetaan kahteen konesaliin. Niitä käytetään kampuksilta nopeiden yhteyksien yli. Vikatilanteessa käyttäjä pääsee mobiililaajakaistan tai koti-Internet-yhteyden yli suoraan konesalien palveluihin. Sijoittelu vaikuttaa myös kustannuksiin ja henkilökunnan määrään.

Hallinnan helppous on avaintekijä kun määritellään järjestelmään uusia yhteyksiä ja tehdään esimerkiksi palomuurisääntöjä. Hallintakysymykset korostuvat hajautetussa mallissa. Siellä signaloinnilla on merkittävä rooli kaikessa yhteyksien määrittelyssä. Ne olisivat muuten erittäin työläitä ja virheherkkiä kohtia.

Vikojen rajaaminen tiettyyn osaan verkko on oltava helppoa. Selvitettäessä minkä kampuslinkin takaa ongelma tulee, tarvitaan selkeät ohjeet ja tehokkaat keinot esimerkiksi kaikkien kampuslinkkien sulkemiseen kerralla ja niiden avaamiseen yksi kerrallaan.

10.2 Kustannuksien vertailu

Kustannusten vertailun helpottamiseksi reititinvaihtoehtoja on vain kolme. Hinta on laskettu Internetistä löytyneiden verkkokauppojen avulla ja se on suuntaa-antava. Hintaerittely on liitteessä 3.

Arkkitehtuurien kustannusvertailu

Kampus	Keskitetty arkkitehtuuri EUR	Hajautettu arkkitehtuuri EUR
Konesalit	856 000	856 000
Otaniemi	24 500	163 000
Töölö	24 500	163 000
Arabia	24 500	163 000
Lahti	24 500	163 000
Mikkeli	24 500	163 000
Pori	24 500	163 000
Vaasa	24 500	163 000
Yhteensä	1 027 500	1 997 000

Taulukko 4 Arkkitehtuurien kustannusvertailu

Konesalien reitittimissä ei ole eroa arkkitehtuurivaihtoehtojen välillä. Niiden osuus kokonaiskustannuksista on ratkaiseva. Konesalireitittimiin myös kannattaa sijoittaa. Konesalireitittimien ominaisuudet tulevat usein rajoittaviksi tekijöiksi kun verkkoon halutaan uusia palveluita tai verkon suorituskykyä halutaan parantaa.

Kampuskytkinten ja kampusreitittimien porttimäärät on valittu niin lähelle toisiaan kuin mahdollista. Ulospäin menevän liikenteen suorituskykyä rajoittavat vain konesalien reitittimet. Kaikki Internet-liikenne kulkee niiden kautta molemmissa arkkitehtuurimalleissa.

10.3 Asiantuntijahaastattelujen yhteenveto ja vertailu

Kaikki kolme haastateltavaa Otto Kaipio HP:lta, Leo Lähteenmäki Ciscolta ja Juha Oinonen CSC:ltä työskentelevät päivittäin verkkotekniikan parissa. Heidän näkemyksensä olivat pääosin keskenään yhteneviä.

Verkon malliin vaikuttaa olennaisesti mihin palvelut sijoitetaan. Hajauttamalla palveluita voidaan paikallaan pysyviä käyttäjiä palvella hyvin. Käyttäjien liikkuvuuden myös tilanne mut-

kistuu. Palomuuriavaukset hajautettuun palveluun monimutkaistuvat moninkertaisesti. Kyseessä on kuitenkin vain koko yliopistolle tarjottavan palvelun yksi versio. Versioiden määrän kasvu ei helpota verkon eikä palvelun suunnittelua.

Haastateltujen mielestä hajautetussa mallissa sisäverkon reititys pitää hoitaa IGP:llä (OSPF tai IS-IS). Se huolehtii liikenteen uudelleenohjauksen linkin vikaantuessa. Reititys pitää tehdä lähellä palveluja. Kampuksen konesalissa pitää olla reititin, jos siellä on palvelimia. Konesalien reitittimet riittävät, jos malli on keskitetty.

Fyysisen verkon rakenteesta kaikilla oli selkeä ehdotus muuttaa Töölön ja Arabian linkit suoraan konesaleihin. Nykyisessä rengasmuodossa Töölön ja Arabian linkkien välillä on oltava IGP käytössä. Verkon rakenteen muuttaminen kaikkialla samanlaiseksi on perusteltua myös kun palvelut ovat enimmäkseen kahdennettuina kahdessa konesalissa. Toisen konesalin vikaantuessa kaikki liikenne Töölöstä kiertäisi turhaan Arabian kautta ja päinvastoin. Lisäksi kuormantasaus ei toimi luontevasti nykyisellä rengasrakenteella. Liikenteen kohdistumista tulisi myös miettiä. Kulkeeko Arabian ja Töölön välillä liikennettä niin paljon, että sen takia tarvittaisiin oma linkki siihen väliin.

VLAN:ien käyttö kampuslinkkien aiheutti paljon pohdintaa. Liikenteen määrää on vaikea arvioida ja palveluiden sijoittelu on ratkaisevaa voiko VLAN:eja hyödyntää. Useimmissa projekteissa he ovat nähneet käytettävän reititettyjä linkkejä. Niillä on omat rajoituksensa esimerkiksi porttiautentikoinnin kanssa.

Tiivistelmä haastateltavien ajatuksista kysymyksittäin:

1. Missä pisteissä reititetään ja missä on vain kytkimet?
   Reititys pitäisi tehdä palveluiden lähellä. Palveluiden sijoittaminen on perusta verkon suunnittelulle.

2. Mitä reititysprotokollia mielestäsi tulisi käyttää?
   IGP:nä OSPF tai IS-IS. Internetin suuntaan käytetään BGP:tä.

3. Käyttäisitkö VLAN:eja kampuslinkkien yli?
   VLAN:ien käyttö on järkevää kun palvelut on keskitetty.

4. Mihin palvelimet tulisi sijoittaa? Sijoitetaanko kaikki konesaleihin vai osa kampuksille?

Palvelimet on järkevintä sijoittaa vähintään kahteen konesaliin kustannussyistä. Konesalit pitää mitoittaa niin suuriksi, että kolmatta konesalia ei tarvita. Se vaikeuttaa hajauttamista.

5. Miten verkon fyysistä rakennetta voisi kehittää?
   Töölön ja Arabian kampuksien yhteydet pitäisi kytkeä suoraan konesaleihin. Vaasaan voisi hankkia toisen yhteyden.

11 Yhteenveto

11.1 Tulokset

Tutkimuksen tarkoituksena oli vertailla ja selvittää kahden erilaisen verkkoratkaisun vaikutusta Aalto-yliopiston verkkopalveluiden arkkitehtuuriin. Verkon rakenteen valinta on pitkälle periaatteellinen ja valinnassa joudutaan arvioimaan myös henkilökunnan valmiutta suuriin muutoksiin. Kustannusten vaikutus saataviin ominaisuuksiin nähden on suuri. Lisäominaisuudet maksavat paljon ja verkkolaitteiden 10 vuoden elinkaaren aikana tekniikka on kehittynyt hurjasti eteenpäin, eikä takeita ominaisuuksien lisähinnan takaisinmaksusta ole.

Keskeisiä kysymyksiä suunnitteluun ovat:

- Halutaanko rakentaa yhteisiä tutkimusverkkoja yliopistorajojen yli?
- Voidaanko kaikki palvelimet keskittää kahteen konesaliin?
- Ovatko kampuksille menevät linkit riittävän luotettavia?
- Pystytäänkö keskitetyssä mallissa suojautumaan L2-tason liikennemyrskyiltä?

Molempien vaihtoehtojen kanssa päästään hyvään lopputulokseen, mutta ympäröivä maailma pitää suunnitella vastaamaan verkkoa. Valittaessa keskitetty malli pitää olla rohkeutta tuoda kaikki palvelimet konesaleihin ja ilmoittaa kampuksille, että tällainen valinta on tehty ja siihen liittyy riskejä. Käyttäjiä pitää neuvoa miten toimia siinä tilanteessa, että yhteydet kampukselle ovat varayhteyksistä huolimatta poikki.

Hajautetussa mallissa on vain mielikuvitus rajana sille, minkälaisia yhteyksiä voidaan rakentaa. Verkkoyhteistyö on mahdollista yliopistojen välillä jopa Funetin ulkopuolelle. Hajanainen tutkimusryhmä eri yliopistoissa voisi todella saada yhteisen sisäverkon, jossa tehdä tutkimusta ja hyödyntää yhteisiä resursseja. Nopeudet eivät enää ole rajoittava tekijä, kun 10 GE -yhteyksiä käytetään yleisesti yliopistoverkoissa.

Valintaa helpottaa se, että verkon ytimessä olevat reitittimet voivat olla samoja molemmissa malleissa. Näin siirtyminen keskitetystä hajautettuun on mahdollista myöhemmin eikä se aiheuta mainittavasti tarpeettomia hankintoja alkuvaiheessa. Luonteva polku on lähteä liikkeelle keskitetyllä mallilla ja vasta kun sen ominaisuudet todella loppuvat siirtyä hajautettuun malliin.

Tutkimuksessa piti selvittää ja vertailla vaihtoehtoja verkkopalveluiden arkkitehtuuriksi. Tärkein tutkimuskohde oli fyysisen verkon rakenne. Tutkimuksessa selvisi, että siirtyminen keskitetystä reitityksestä hajautettuun ei aiheuta mainittavasti lisäkustannuksia. Kaikki hankitut laitteet soveltuvat muuhunkin käyttöön.

11.2 Tulosten arviointi

Verkon suunnittelu ja rakentaminen on verrattavissa käsialaan. Harvoin kaksi eri ihmistä päätyy täysin samaan ratkaisuun, ellei ennalta ole rajoitettu vaihtoehtoja merkittävästi. Ratkaisevia asioita ovat kunnianhimo ja kuinka vapaasti asioita pitää pystyä tekemään?

Miten tutkijat ja opiskelija kokevat verkon paranevan jos valitaan keskitetty malli? Heidän on ainakin helpompi ymmärtää miten järjestelmä toimii. Näyttämällä verkon kuvan ja osoittamalla, että piuha on poikki tuosta jokainen voi käsittää miksi yhteydet eivät toimi. Hajautetussa mallissa rakenne voi olla niin monimutkainen, että vain muutama henkilö voi vian ylipäätään selvittää.

Yksinkertainen on kaunista, pätee myös verkonrakennuksessa. Yksinkertaiseen verkkoon uskaltaa tehdä muutoksia ja päivityksiä pienemmällä valmistelulla ja suunnittelulla. Testausta varten on mahdollista pitää laitteita testilaboratoriossa. Testilaboratoriossa voi harjoitella vikatilanteita varten ja kouluttaa uusia työntekijöitä.

Tuloksien perusteella nykyinen verkon rakenne palvelee hyvin molempia vaihtoehtoisia ratkaisuja. Ainoastaan linkki Arabian ja Töölön välillä on hieman kyseenalainen. Jos sen lisäksi saisimme varayhteydet suoraan molempiin konesaleihin, malli olisi erinomainen. Töölön ja Arabian linkkiä voi hyödyntää tehokkaimmin hajautetun reitityksen mallissa.

Siirryttäessä keskitettyihin työasemapalveluihin liikenteen profiili väistämättä muuttuu. Kotihakemistojen ja muiden verkkohakemistojen käyttö lisääntyy ja vierekkäiset koneet eivät enää liikennöi juuri lainkaan keskenään. Käyttäjät liikkuvat koneidensa kanssa paljon enemmän ja vaativat myös palveluja. Uudet kannettavat tietokoneet on varustettu 3G-korteilla ja kampuksilla on erinomaiset langattoman verkon palvelut. Liikkuvuutta tuetaan nykytekniikan äärirajoille asti.

Molemmissa ratkaisuissa on paljon hyviä puolia ja kohtuullisesti huonoja puolia. Valinta on paljon helpompi tehdä kun tiedetään miten palvelut ja palvelimet sijoitetaan 5 vuoden kuluttua? Keskitetystä reitityksestä päästään aina hajautettuun ilman suuria ylimääräisiä kuluja.

Tutkimuksen toistaminen voisi johtaa erilaiseen tulokseen. Haastattelijan kysymykset ja haastateltavan omakohtaiset kokemukset vaikuttavat paljon tuloksiin. Täysin samaan tulokseen tuskin kukaan olisi päätynyt. Erilaisia toteutusvaihtoehtoja on paljon.

Arkkitehtuurimalleiksi tutkimukseen valittiin keskitetty ja hajautettu. Niiden välistä löytyy lukematon määrä erilaisia vaihtoehtoja. Keskitetty malli on verkon minimi ja hajautettu malli on maksimi. Näiden mallien valinta perustuu siihen ajatukseen, että toteutuksessa voi tarvittaessa hyödyntää ominaisuuksia molemmista malleista. Riittävän erilaiset mallit korostavat eroja riittävästi ja antavat kuitenkin käsityksen mallien välimaastossa olevista vaihtoehdoista.

Tuloksen luotettavuutta on vielä vaikea arvioida. Kaikilla haastatelluilla oli hyvin samanlaiset näkökulmat ja olennaisia suuria eroja ei ole. Haastateltavien määrän kasvattaminen ei välttämättä vaikuta lopputulokseen. Kaikkien haastateltujen mielipiteet olivat hyvin samansuuntaisia.

Samoilla lähtötiedoilla ja rajauksella joku muu voisi päätyä hyvin samanlaiseen tulokseen. Polku vie verkkoja hyödyntävien palvelujen kautta liikenteen ohjautumisen kautta käyttötilanteiden tutkimiseen. Vaihtoehtoja on valtavasti ja lopputuloksessa näkyisi varmasti erilaisia teknisiä ratkaisuja.

Arkkitehtuurimalleja on kymmeniä, mutta hajautus ja keskitys ovat luontevat ääripäät. Keskitys on hinnaltaan erittäin edullinen ja helposti ymmärrettävä. Hajautetussa arkkitehtuurimallissa tulee väistämättä paljon kustannuksia. Keskitetyn mallin suurin ongelma on liikenteen kopioituminen esimerkiksi multicastin tapauksessa linkeille useampaan kertaan.

11.3 Tulosten hyödyntäminen

Diplomityön tuloksia voi suoraan hyödyntää suunniteltaessa Aalto-yliopiston verkkopalveluiden arkkitehtuuria viisi vuotta eteenpäin. Merkittävimmät puutteet tällä hetkellä ovat Multicast-tuen puute, 802.1X porttiautentikoinnin puute ja palveluiden hajanaisuus.

Multicastin tuki auttaisi kehittämään videoluentoja ja niiden tallentamista. Multicastien toimimattomuus johtaa siihen, että kukaan ei halua eikä pysty asiaa myöskään tutkimaan. Tek-

niikan hinnan laskeminen tekisi mahdolliseksi nauhoittaa valtaosa luennoista ja lähettää niitä suorana koko yliopistoverkkoon.

Porttiautentikointi 802.1X helpottaisi neuvotteluhuoneiden ja aulojen verkon käyttöä, kun kaikki rasioihin joissa on merkintä X voi laittaa koneen kiinni. Vieraat saavat vierailijaverkon ja yliopiston koneet pääsevät omaan verkkoonsa. Tarvittava tekniikka on jo olemassa, mutta tahto puuttuu.

11.4 Jatkotutkimuksia

Multicastin käyttö opetuksen välittämiseen ja nauhoittamiseen olisi monelle opiskelijalle suuri edistysaskel. Tarvittaessa opetus voisi olla kaksisuuntaista multicastin keinoin. Opiskelijat voisivat halutessaan esittää kysymyksiä ja osallistua omilla kanavillaan.

Käytännön toteutuksia pitäisi etsiä kirjallisuudesta ja tehdä kokeita laboratoriossa. Suuren verkon testaaminen muutamalla laitteella ei anna täyttä kuvaa todellisuudesta, mutta pahimmat ajatusvirheet sieltä löytyvät nopeasti.

Yliopistojen välistä BGP VPLS:ää pitäisi tutkia tarkemmin. Sellaista palvelua ei ole tähän mennessä Suomessa toteutettu. Sen käyttöönotto vaatii huolellista selvitystä, mutta toimiessaan toisi paljon lisäarvoa tutkimusryhmille.

Lähdeluettelo

[1] Aalto-yliopisto, 2010. Verkkodokumentti. Päivitetty 21.5.2010. Viitattu 21.5.2010. Saatavissa: http://www.aalto.fi/

[2] Opetusministeriö, 2007. Hallituksen iltakoulu 21.11.2007. Yliopistojen taloudellisen ja hallinnollisen aseman uudistaminen ja innovaatioyliopiston perustaminen. Verkkodokumentti. Päivitetty 21.11.2007. Viitattu 10.5.2010. Saatavissa: http://www.minedu.fi/export/sites/default/OPM/Koulutus/koulutuspolitiikka/Hankkeet/Yliopistolaitoksen_uudistaminen/liitteet/Iltakoulu_21__11.2007.pdf

[3] Aalto-yliopiston IT-palvelukeskus, 2010, Verkkodokumentti. Päivitetty 11.2.2010. Viitattu 4.5.2010. Saatavissa: http://www.aalto.fi/fi/about/organization/services/it/

[4] Teknillisen korkeakoulun ja Helsingin kauppakorkeakoulu,2008 Tietohallinnon johtoryhmän pöytäkirja 3/2008. Verkkodokumentti. Päivitetty 12.6.2008. Viitattu 15.5.2010. Saatavissa: https://wiki.aalto.fi/download/attachments/25832338/IT-johtokunta_3_2008_liite5.pdf?version=1&modificationDate=1223627139000

[5] Aalto-yliopisto, Tietohallinto, 2009. Aalto-yliopiston työasemapolitiikka. Aalto-yliopiston sisäisillä sivuilla. Verkkodokumentti. Päivitetty 31.8.2009. Viitattu 6.5.2010. Saatavissa Aalto-yliopiston intranetistä: https://inside.aalto.fi/download/attachments/4392510/AALTO+YLIOPISTON+TYOASEMAPOLITIIKKA.pdf?version=4&modificationDate=1259936019000

[6] Aalto-yliopisto, 2010. Aalto-yliopiston korkeakoulut ja yksiköt. Päivitetty 20.5.2010. Viitattu 21.5.2010. Saatavissa: http://www.aalto.fi/fi/about/organization/schools/

[7] Aalto-yliopisto, Tutkimus, 2010. Verkkodokumentti. Päivitetty 21.5.2010. Viitattu 22.5.2010. Saatavissa: http://www.aalto.fi/fi/research/

[8] IEEE 802.3 Ethernet Working Group, Verkkodokumentti. Päivitetty 3.4.2010. Viitattu 11.5.2010. Saatavissa: http://www.ieee802.org/3/

[9] Aalto-yliopisto, 2010. Langattomien verkkojen käyttöehdot. Verkkodokumentti. Päivitetty 22.4.2010. Viitattu 10.5.2010. Saatavissa: http://www.aalto.fi/fi/about/organization/services/it/guidelines/aalto_open-verkko/

[10] Terena, 2010, Eduroam, Verkkodokumentti. Päivitetty 5.1.2010. Viitattu 13.5.2010. Saatavissa: http://www.eduroam.org/

[11] Adobe, 2010, Adobe connect. Verkkodokumentti. Päivitetty 2010. Viitattu 13.5.2010. Saatavissa: http://www.adobe.com/products/acrobatconnectpro/

[12] ITU-T H.323 Implementors' Guide for Recommendations of the H.323 System. Verkkodokumentti. Päivitetty 3.12.2009. Viitattu 12.5.2010. Saatavissa: http://www.itu.int/rec/T-REC-H.323/e

[13] IETF, 2010 IANA Guidelines for IPv4 Multicast Address Assignments, 3/2010. Päivitetty 3/2010.

Viitattu 14.5.2010. Saatavissa: http://tools.ietf.org/html/rfc5771

[14] Aalto-yliopisto opetus, 2010. Verkkodokumentti. Päivitetty 20.5.2010. Viitattu 21.5.2010. Saatavissa: http://www.aalto.fi/fi/studies/

[15] CSC, 2010, Funet valopolku. Viitattu 17.5.2010. Saatavissa: http://www.csc.fi/csc/julkaisut/esitteet/funet_valopolku_esite_tekninen

[16] CSC 2010, Funet-verkon tila. Viitattu 17.5.2010. Saatavissa: http://www.csc.fi/hallinto/funet/status

[17] The Internet Society, 2003. RFC, Internet Small Computer Systems Interface (iSCSI). Verkkodokumentti. Päivitetty 4.2004. Viitattu 18.5.2010. Saatavissa: http://tools.ietf.org/html/rfc3720

[18] Juniper, 2010. Verkkodokumentti. Päivitetty 2010, Viitattu 15.5.2010. Saatavissa: http://www.juniper.net Cisco, 2010. Verkkodokumentti. Päivitetty 2010, Viitattu 15.5.2010. Saatavissa: http://www.cisco.com

[19] FCIA, Fibre Channel Industry Association, 2010. Verkkodokumentti. Viitattu 16.5.2010. Saatavissa: http://www.fibrechannel.org/

[20] IETF, The Transport Layer Security (TLS) Protocol Version 1.2, 2008. Verkkodokumentti. Päivitetty 8/2008. Viitattu 17.5.2010. Saatavissa: http://tools.ietf.org/html/rfc5246

[21] CSC, 2010. Ekotehokkaat ja turvalliset konesaliratkaisut. Verkkodokumentti. Päivitetty 30.3.2010. Viitattu 14.5.2010. Saatavissa: http://www.csc.fi/sivut/e-infra/ekotehokkaatkonesalit

[22] Eaton, 2010. Data Center ja kiinteistö UPS:it. Verkkodokumentti. Päivitetty 2010. Viitattu 4.5.2010. Saatavissa: http://powerquality.eaton.com/Products-services/Backup-Power-UPS/Data-Center-Facility/default.aspx

[23] Oy Ekströmin Koneliike Ab, Generaattorin ohjauslogiikka. Verkkodokumentti. Viitattu 10.5.2010. Saatavissa: http://www.ekstrom.fi/site/doc/106.pdf

[24] HP, Boot from SAN, 2010. Verkkodokumentti. Päivitetty 2010. Viitattu 12.5.2010. Saatavissa: http://www.compaq.com/storage/networking/bootsan.html

[25] HP 802.1X solution, 2009. Verkkodokumentti. Päivitetty 2009. Viitattu 16.5.2010. Saatavissa: http://www.hp.com/rnd/pdf_html/guest_vlan_paper.htm#802.1X_solution

[26] Wi-Fi Alliance. WPA2, 2010. Verkkodokumentti. Päivitetty 2010. Viitattu 17.5.2010. Saatavissa: http://www.wi-fi.org/knowledge_center/wpa2

[27] Network Working group, LDAP RFC4511, 6/2006. Päivitetty 6/2006. Viitattu 8.5.2010. Saatavissa: http://www.rfc-editor.org/rfc/rfc4511.txt

[28] CSC, 2010. Funet-palvelut. Verkkodokumentti. Viitattu 14.5.2010 Saatavissa: http://www.funet.fi

[29] Network Working Group, 1/2001. Multiprotocol Label Switching Architecture. Päivitetty 1/2001. Viitattu 13.5.2010. Saatavissa: http://tools.ietf.org/html/rfc3031

[30] Juniper 2009, LDP-BGP Interworking, Verkkodokumentti. Päivitetty 21.12.2009. Viitattu 7.5.2010. SAatavissa:

http://kb.juniper.net/library/CUSTOMERSERVICE/GLOBAL_JTAC/technotes/2000282-en.pdf

[31] Network Working Group, 1990. IS-IS RFC 1195. Päivitetty 12/1990. Viitattu 4.5.2010. Saatavissa: http://tools.ietf.org/html/rfc1195

[32] IETF 12/2001. RSVP-TE: Extensions to RSVP for LSP Tunnels. Päivitetty 1/2001. Viitattu 3.5.2010. Saatavissa: http://www.ietf.org/rfc/rfc3209.txt

[33] Juniper, 2010. Bidirectional Forwarding Detection Overview. Verkkodokumentti. Viitattu 10.5.2010. Saatavissa: http://www.juniper.net/techpubs/en_US/junose11.0/information-products/topic-collections/swconfig-ip-services/id-28095a.html

[34] Network working group, 3/1995. A Border Gateway Protocol 4 (BGP-4). Verkkodokumentti. Päivitetty 3/1995. Viitattu 6.5.2010. Saatavissa: http://www.ietf.org/rfc/rfc1771.txt

[35] Juniper 2/2009, LDP-BGP VPLS Interworking. Verkkodokumentti. Päivitetty 2/2009 Viitattu 15.5.2010. Saatavissa: http://www.juniper.net/us/en/local/pdf/whitepapers/2000282-en.pdf

[36] The Internet Society, 2004. RFC 3768 – Virtual Router Redundancy Protocol. Verkkodokumentti Päivitetty 4/2004. Viitattu 16.5.2010. Saatavissa: http://tools.ietf.org/html/rfc3768

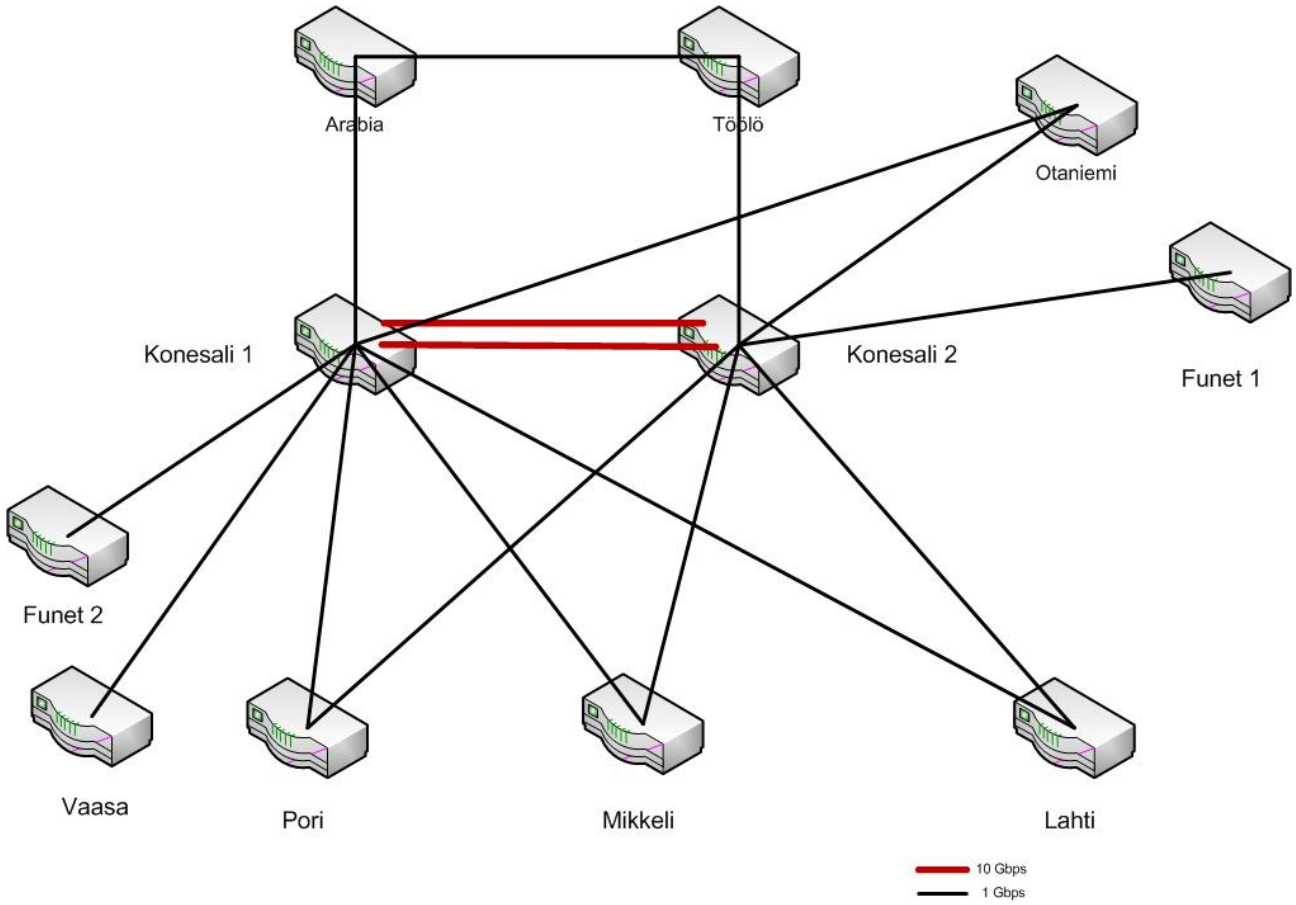
[37] Nortel White paper, 2006. Ethernet now offers the most comprehensive OAM for packet-based solutions. Päivitetty 2006, Viitattu 19.5.2010. Saatavissa: http://www.nortel.com/solutions/collateral/nn119660.pdf

Liite 1 - Asiantuntijahaastattelulomake

Yritys, Haastateltavan nimi

Aalto-yliopiston verkkopalveluiden arkkitehtuuri

Verkon fyysinen rakenne



Kuva 13 Verkon fyysinen rakenne

Kuvassa näkyvät verkkoyhteydet konesaleista kampuksille. Kaavio on suuntaa-antava ja sitä pitää ajatella vain fyysisten yhteyksien kuvauksena. Verkkoyhteydet on toteutettu yksimuoto-valokaapelilla tai valopoluilla (CWDM).

Kaikkia rakenteita voi kommentoida ja ehdottaa muutettavaksi.

Käyttäjämäärien suuruusluokka:

Arabia: 450 henkilökuntaa ja 2000 opiskelijaa

Töölö: 450 henkilökuntaa ja 3500 opiskelijaa

Otaniemi: 3500 työntekijää ja 14500 opiskelijaa

Lahti: 50 työntekijää

Mikkeli: 50 työntekijää ja 200 opiskelijaa

Pori: 50 työntekijää

Vaasa: 20 työntekijää

Aliverkkojen määrä

Jokaisella kampuksella on työasemia ja muita laitteita varten vähintään 5 aliverkkoa. Aliverkkojen kokonaismäärä yhteensä kaikilla kampuksilla on alle 1000.

Kysymykset

6. Missä pisteissä reititetään ja missä on vain kytkimet?
7. Mitä reititysprotokollia mielestäsi tulisi käyttää?
8. Käyttäisitkö VLAN:eja kampuslinkkien yli?
9. Mihin palvelimet tulisi sijoittaa? Sijoitetaanko kaikki konesaleihin vai osa kampuksille?
10. Miten verkon fyysistä rakennetta voisi kehittää?

Kiitos ajastasi

Tommi Saranpää

050-5897883

Liite 2 – Asiantuntijahaastattelut

Asiantuntijahaastattelu Kaipio

HP, Otto Kaipio 14.5.2010

1. Missä pisteissä reititetään ja missä on vain kytkimet?

Reititys voidaan hoitaa sijoittamalla kaksi reititintä molempiin konesaleihin. L2-verkko olisi ehkä liian iso Otaniemen kampuksen suuresta konemäärästä johtuen. Reititystä pitäisi hajauttaa kampuksille. Hajautuksen tarve riippuu siitä ovatko kaikki palvelimet konesaleissa, vai onko niitä myös kampuksilla? Sijoittamalla kaikki palvelimet konesaleihin L2-verkko on perusteltua. Näin liikenne kulkee vain kertaalleen kampukselle menevällä linkillä työasemien ja palvelinten välillä. Tilanteessa jossa reititys on keskitetty ja palvelimet hajautettu, kävisi liikenne kääntymässä konesalissa tullakseen takaisin kampukselle. Hallinnan kannalta on järkevämpää reitittää vain muutamissa pisteissä

2. Mitä reititysprotokollia mielestäsi tulisi käyttää?

OSPF sisäisenä reititysprotokollana (IGP) ja BGP ulospäin.

3. Käyttäisitkö VLAN:eja kampuslinkkien yli?

Verkko on järkevää rakentaa ensisijaisesti reititettynä. VPLS:n käyttöä tulisi harkita? Kampusten reititys voidaan hoitaa reitittävillä kytkimillä, jotka tukevat MPLS:ää. Pääreitittiminä voisivat olla Ciscon Nexus 7000 tai 6500 sarja. Myös HP hiljattain ostamalta H3C:ltä löytyy ytimeen sopivia laitteita.

4. Mihin palvelimet tulisi sijoittaa? Sijoitetaanko kaikki konesaleihin vai osa kampuksille

Reitityksen kannalta edullisin ratkaisu on sijoittaa palvelimet konesaleihin. L2-verkko vaatisi sen, että palvelimet ovat vain konesaleissa. VLAN:ista toiseen reititys kulkisi edestakaisin konesalien ja kampuksen väliä.

5. Miten verkon fyysistä rakennetta voisi kehittää?

Töölön ja Arabian välinen yhteys on kyseenalainen. Järkevämpää olisi tehdä toinen suora konesaliyhteys. Kustannuksien kannalta on järkevää keskittää kaikki palvelimet konesaleihin ja huolehtia riittävän luotettavista yhteyksistä kampuksille. Tarvitaan riskianalyysi siitä kuinka varma linkki kampusten välillä on? Yhdistelmä keskitetystä ja hajautetusta palvelusta on kaikkein hankalin, koska linkin katketessa voi osa palveluista olla aina saavuttamattomissa. Esimerkiksi tilanne, jossa kotihakemisto on kampuksella ja tulostukset kulkevat konesalin kautta. Toinen on aina poikki, jos kampuksen linkki on poikki. Varayhteytenä voi käyttää kotiyhteyttä (ADSL tms.) ja VPN:ää silloin kun kaikki on keskitetty.

Asiantuntijahaastattelu Lähteenmäki

Cisco, Leo Lähteenmäki 17.5.2010

1. Missä pisteissä reititetään ja missä on vain kytkimet?

Reitityksen sijoitus riippuu siitä, mitä palveluita halutaan käyttää. Puhtaassa IP-verkossa voidaan reititys sijoittaa talokytkimiin. Reitittämällä kampuksilla, spanning tree protokollan tarve poistuu. Redundanssi verkkoyhteyksissä voidaan hoitaa IGP reititysprotokollilla. Esimerkiksi käyttäen OSPF:ää. L2-tason yhteyksiä on käytetty asiakasprojekteissa, kun jokin palvelu on siirretty palveluntarjoajan verkkoon.

2. Mitä reititysprotokollia mielestäsi tulisi käyttää?

OSPF ja BGP, IS-IS on suosittu operaattoripuolella.

OSPF ei ole ongelma suurissakaan verkoissa. OSPF on tuettuna lähes kaikissa reitittävissä laitteissa. IS-IS:ää ei saa kaikkiin laitteisiin.

3. Käyttäisitkö VLANeja kampuslinkkien yli?

Kyse on yleensä pakosta eli esimerkiksi vmware vmotion. Spanning tree protokolla on aina tähän asti ollut ainoa vaihtoehto L2-verkoissa. Uudet reitittimet tukevat Multi chassis -kanavatekniikoita. Konesali 1 ja 2 reitittimistä voidaan muodostaa yksi looginen reititin. Esimerkkinä Ciscon 6500 sarja tukee Cisco Virtual Switching Systemiä (VSS). Nexus sarja tukee Virtual Port Channelia (VPC). Kaksi Nexusta säilyisivät erillisinä laitteina, mutta voivat

ottaa vastaan kanavan kahdesta kytkimestä. Kanavasta otsikkotietojen pohjalta tehdään tiiviste ja sen perusteella liikenne ohjataan oikeaan paikkaan. Reitityksen kuormantasaus tekniikoita ovat GLBP, VRRP ja HSRP. Orpojen käsittely pitää ratkaista siinä tilanteessa, että johonkin kohteeseen on vain yksi linkki. Split brain -tilanteessa reitittimien välinen yhteys on poikki, mutta jollain tavalla reitittimien pitää saada tieto onko toinen hengissä. Suunnitelma B on estää matalamman prioriteetin laitetta palvelemasta, kunnes reitittimien väliset linkit jälleen toimivat.

4. Mihin palvelimet tulisi sijoittaa? Sijoitetaanko kaikki konesaleihin vai osa kampuksille

Konsolidointi on ollut jo 10 vuotta selkeä suuntaus. Pilvipalveluissa työkuormat ja kapasiteetit eriytyvät toisistaan. Kuormat siirtyvät virtualisointitekniikoiden avulla paikasta toiseen. Kaksi konesalia riittää normaalisti. Yksi konesali on liian vähän. Kolmas tulee yleensä rakennettavaksi kapasiteetin loppuessa. Suuruuden ekonomia toimii konesaleissa erinomaisesti.

5. Miten verkon fyysistä rakennetta voisi kehittää?

Verkkosuunnittelun näkökulmasta Arabian ja Töölön väliset kuituyhteydet pitäisi kytkeä suoraan konesaleihin. Nykyinen rakenne on hyväksyttävä, jos käytössä on IGP. L2-tason verkkoratkaisut ovat mahdollisia, jos linkki on riittävän nopea. Hitaammilla yhteyksillä voi käyttää kahden pisteen välistä L3 -yhteyttä konesalin ja kampuksen välillä. L2-yhteyden voi tehdä tarvittaessa myöhemmin.

Verkon pilkkomisen eritasoisiin verkkoihin kuten oppilasverkot, hallintoverkot jne. voidaan toteuttaa VRF-lite:lla (VPN Routing and Forwarding instances lite). Siinä tekniikassa virtualisoidaan reititystaulu. Tämä toimii hyvin kun segmenttejä ei ole paljon. Kaikki aliverkot pitää jakaa kaikkiin laitteisiin. Laitteet voivat olla joko VRF-liteä tukevia kytkimiä tai reitittimiä.

Asiantuntijahaastattelu Oinonen

CSC, Juha Oinonen 18.5.2010

1. Missä pisteissä reititetään ja missä on vain kytkimet?

Funetin rajalla on luontevaa reitittää. Loppu riippuu siitä miten verkon haluaa rakentaa. Käsitys pelkästä VLAN-toteutusvaihtoehdoista on rajoittunut, eikä siitä ole CSC:llä kokemuksia. Esimerkiksi hallinnon pitää olla eriytettynä opiskelijoista. Erilaisia verkkoja ovat tutkimusverkko, vierailijaverkko ja akateeminen verkko.

Palvelimien sijoittelu on ratkaisevaa. Siellä missä on paljon liikennettä pitää reitittää. Liikenne jakaantuu pääosin kulkeakseen palvelimiin tai Internetiin. Internetin suuntaan tarvitaan pääyhteys ja varayhteys. Kampusten välinen liikenne ja sen toteutus on periaatepäätös.

Miten paljon reititystä tarvitaan varayhteyksien toteuttamiseen? Liikenteen voisi hoitaa ilman reititystä kampuksilla esimerkiksi siten, että kampuslinkeillä käytetään VLAN:eja.

2. Mitä reititysprotokollia mielestäsi tulisi käyttää?

Funetiin BGP, IPv4 ja IPv6 maailmaa varten pitää miettiä IGP vaihtoehtoja. OSPF tuki laitevalmistajilla. IS-IS tuki IPv6 maailmassa.

3. Käyttäisitkö VLAN:eja kampuslinkkien yli?

Kyllä. Molemmilla on puolensa. Miten palomuuraus hoidetaan? Onko palomuurien hallinta keskitettyä? Jos kyllä, niin palomuurit voidaan keskittää. Palomuurien ylläpito on raskaampaa kuin VLAN:ien ylläpito.

Kuormituspiikkitilanteissa VLAN:it syövät toisiltaan kaistan. Löytyykö VLAN:eista liikenteen rajoitus ominaisuutta.

4. Mihin palvelimet tulisi sijoittaa? Sijoitetaanko kaikki konesaleihin vai osa kampuksille?

Reitityksen ja palvelimien sijoittelu pitää tasapainottaa. Palvelimia ei kannata hajauttaa, jos reititystä ei hajauta. Monimutkaisuutta tulee muutenkin riittävästi eli sitä kannattaa karsia.

5. Miten verkon fyysistä rakennetta voisi kehittää?

Vaasassa ei ole varayhteyttä. Yksi vaihtoehto olisi muuttaa Porin toinen yhteys Vaasaan. Onko Töölössä ja Arabiassa palvelimia ja kuinka suuri on liikennemäärä niiden välillä?

Liite 3 – Hintaerittely laitteistoista

Konesalireititin

Juniper MX960:

1. 40 SFP 1 GE
2. 200 10/100/1000 Mbps RJ45
3. 48 SFP+ 10 GE
4. Tarvittavat lisenssit

Yhteensä 428 000 EUR. Alla on hintaerittely ja komponenttilista.

	kpl	EUR	Yhteensä
MX960-PREMIUM-AC Base system with redundant RE-2000, SCB, and power	1	30000	30000
JUNOS-WW JUNOS Internet Software Worldwide Version	1	3000	3000
JS-IPv6 IPv6 Support on JUNOS	1	0	0
MX-MPC2-3D 2xTrio Chipset MPC, port queuing, price includes full scale L2/L2.5 and reduced scale L3 features	6	17000	102000
S-MPC-3D-PQ-ADV-R License, per slot, to support full scale L3 route and L3 VPN on port queuing MPCs	6	7000	42000
MIC-3D-20GE-SFP 20x10/100/1000 MIC for MX, requires optics sold separately	2	3000	6000
MIC-3D-40GE-TX 40x10/100/1000 RJ-45 full height MIC (fixed optics)	5	4000	20000
MPC-3D-16XGE-SFPP-R-B16x10GE line card bundle, includes full scale L3, L2 and L2.5 features	3	75000	225000
Yhteensä			428000

Kampusreititin

Juniper MX960:

1. 20 SFP 1 GE
2. 40 10/100/1000 Mbps RJ45
3. 16 SFP+ 10 GE
4. Tarvittavat lisenssit

Yhteensä 163 000 EUR

	kpl	EUR	Yhteensä
MX960-PREMIUM-AC Base system with redundant RE-2000, SCB, and power	1	30000	30000
JUNOS-WW JUNOS Internet Software Worldwide Version	1	3000	3000
JS-IPv6 IPv6 Support on JUNOS	1	0	0
MX-MPC2-3D 2xTrio Chipset MPC, port queuing, price includes full scale L2/L2.5 and reduced scale L3 features	2	17000	34000
S-MPC-3D-PQ-ADV-R License, per slot, to support full scale L3 route and L3 VPN on port queuing MPCs	2	7000	14000
MIC-3D-20GE-SFP 20x10/100/1000 MIC for MX, requires optics sold separately	1	3000	3000
MIC-3D-40GE-TX 40x10/100/1000 RJ-45 full height MIC (fixed optics)	1	4000	4000
MPC-3D-16XGE-SFPP-R-B16x10GE line card bundle, includes full scale L3, L2 and L2.5 features	1	75000	75000
Yhteensä			163000

Kampuskytkin

HP Procurve 8212zl:

1. 12-paikkainen kehikko ja virtalähteet
2. 92 10/100/1000 Mbps Power Over Ethernet RJ45
3. 28 SFP 1 GE
4. 16 SFP+ 10 GE

Yhteensä 24 500 EUR

	kpl	EUR	Yhteensä
J9448A HP PROCURVE 5412ZL-96G-POE+ SWITCH (Hinta sisältää 2 x J9307A ja 1 x J9308A. Hinnat erikseen alla)	1	9000	9000
J9307A HP ProCurve 24-Port 10/100/1000 PoE+ zl Module	0	2700	0
J9308A HP ProCurve 20-Port 10/100/1000 PoE+ and 4-Port Mini-GBIC zl Module	0	2700	0
J9309A HP ProCurve 4-Port 10GbE SFP+ zl Module	4	2700	10800
J9306A HP PROCURVE SWITCH ZL 1500W POE+ PSU	2	650	1300
J9092A HP ProCurve Switch 8200zl Management Module	1	3400	3400
Yhteensä			24500